NTP Software QFS®

Family of Products

User Manual

Revision 2.1 - July 2015

This manual details the method for using NTP Software QFS® Family of Products from an administrator's perspective. Upon completion of the steps within this document, NTP Software QFS Family of Products will be used to manage your enterprise community successfully.

Table of Contents

Copyright © 2000-2015 NTP Software

Executive Summary

Thank you for your interest in the NTP Software QFS® Family of Products. NTP Software QFS controls storage for millions of users worldwide. NTP Software QFS Family of Products extends our best-of-breed technology, allowing you to manage Windows® and NAS-hosted storage as a seamless whole.

Given the architecture of your NetApp® Filer®, EMC® CIFS Server, EMC® Isilon, Dell® NAS or Hitachi® NAS, NTP Software QFS does its job remotely. Part of the NTP Software QFS Family of Products, NTP Software QFS uses a connector service to create a bridge and include Filers/CIFS Servers/Hitachi NASs/Isilon/Dell NASs as full participants in storage environments controlled by NTP Software QFS. In light of this fact, you will need to install the NAS/EMC/Hitachi/NRT connector on one of the Windows Server® 2008, or Windows Server® 2012 machines in your environment. This may be an existing server or workstation or a standalone system.

To be managed by NTP Software QFS, version 6.5 or later (excluding versions 7.1) of the Data ONTAP® operating system for Filers, or version 5.6.49.3 or later of the DART operating system for CIFS Servers, or version 6.1.1684.18 of or version 6.1.1684.18 of the HOS operation system for Hitachi NASs is required.

NTP Software QFS Family of Products can be used to manage Windows servers, Filers, CIFS Servers, Hitachi NASs, Filer clusters, CIFS Server clusters, and Hitachi NAS clusters, EMC Isilons, Dell NASs, or any combination of these systems.

NTP Software QFS imposes no restrictions on how you organize or manage your storage. You can impose policies on individual directories, users, and/or groups of users. Unlike QFS for NAS, QFS for Windows has the ability to set quotas on files.

NOTES:

- Version 5.6.49.3 or later of the DART operating system is the minimum for CIFS support.
- Version 7.3 or later of the Data ONTAP operating system is required for NFS support.
- If QFS is installed on a Windows Server 2008 or later, it is then recommended to upgrade to Data ONTAP version 7.3.3 or later
- Version 8.2 or later of the Data ONTAP operating system is required for supporting Cluster mode NetApp Filer.
- With HOS operation system for Hitachi NASs - If QFS is installed on a Windows Server 2008 or newer, then the HOS version must be 7.0.2010.00 or later.
- If you want to use email-based messaging and notifications, access to an email

Copyright © 2000-2015 NTP Software

server is required.

To install NTP Software QFS on Windows, a login with administrator rights is needed. You will be installing three different services: the NTP Software Smart Policy Manager™ service, the QFS service, and the NAS/EMC/Hitachi/NRT connector service.

The NTP Software Smart Policy Manager service should be installed with a domain user account as its service account so that it can communicate with your mail system and other storage servers with which it may share policies. The QFS service requires a domain user account with local administrative rights on the Filer, EMC CIFS Server, Hitachi NAS, EMC Isilon, or Dell NAS. The QFS connector service uses this account as well.

Your hardware should be appropriate for the services running on each machine.

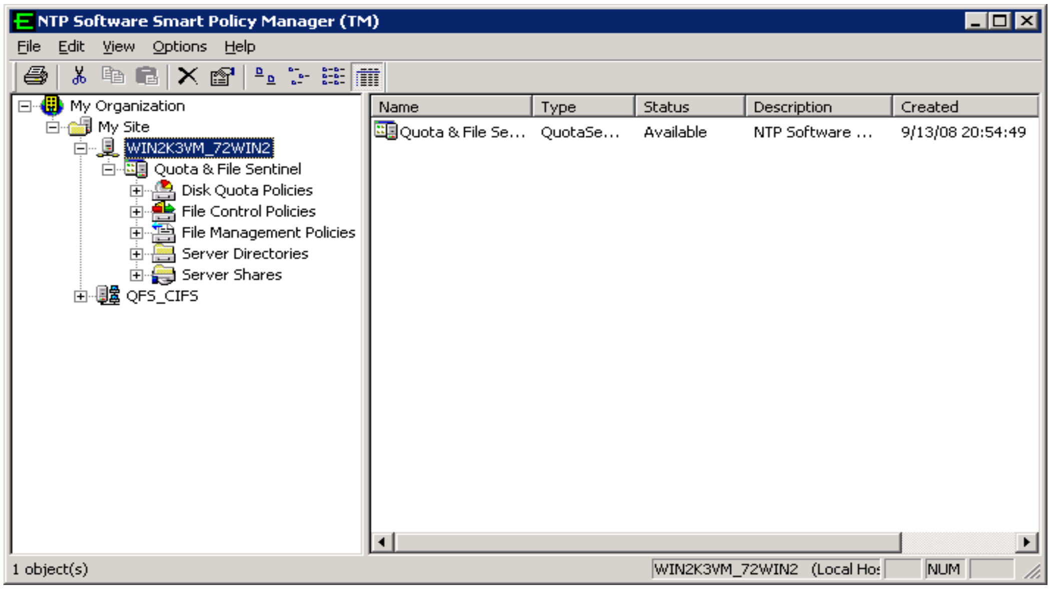
NTP Software Smart Policy Manager™ Overview

The first step in using NTP Software QFS is to lay out your strategy for quota policies and file control policies. Before doing this, though, let's look at our underlying policy-based rules engine: NTP Software Smart Policy Manager.

NTP Software Smart Policy Manager allows you to organize your storage resource management policies in a way that is a unique fit to your organization. If you manage by geography or administrative unit, you can use that plan. If you manage by class of machine, that approach works just as well. Often, companies use a mixed mode — perhaps geography, department, and type of machine. NTP Software Smart Policy Manager has the flexibility you need to make using NTP Software QFS simple.

Once you have laid out your management structure, NTP Software Smart Policy Manager provides policy replication throughout your enterprise. It allows machines to access the policies in their containers and inherit policies from all levels above that point in your hierarchy. You no longer need to configure and manage the machines on your network one by one.

As you start to configure the software you have installed, begin with the top-level container under the root organization (in the following example, My Site). This is the Global Network configuration, whose container we created during installation.


NTP Software Smart Policy Manager (TM)
File Edit View Options Help

- My Organization
  - My Site
    - WIN2K3VM_72WIN2
      - Quota & File Sentinel
        - Disk Quota Policies
        - File Control Policies
        - File Management Policies
        - Server Directories
        - Server Shares
    - QFS_CIFS

Name	Type	Status	Description	Created
Quota & File Se...	QuotaSe...	Available	NTP Software ...	9/13/08 20:54:49

1 object(s)
WIN2K3VM_72WIN2 (Local Ho:
NUM

NOTE: With QFS for Windows, the application name in the hierarchy is **NTP Software QFS** and not **Quota & File Sentinel** as with QFS for NAS.

Preparing the QFS Machine

To prepare the QFS machine, you need to add HOSTS and LMHOSTS file entries that include the IP address and the CIFS server name of the EVS. The IP address should be the one of the dedicated network. It is recommended that the QFS software and the Filer be connected via a dedicated/private network. If it is connected to a private network, then the HOSTS and LMHOSTS file entries need to be modified. If using the public network, then the companies DNS infrastructure should be sufficient.

Important: The logon account used to register with the NetApp Filer (the account that will be assigned to the QFS connector service) needs to be a member of the Filer's local administrator group.

Preparing NetApp Filers

Refer to this section only if you have NetApp Filers attached to your environment. If you do not have a NetApp Filer, you should not apply the instructions specified in this section.

Enabling the fpolicy Management Service (NetApp Filers)

NTP Software QFS requires NetApp Filers to run Data ONTAP version 6.5 or later (excluding versions 7.1).

NOTES:

- Versions 8.0 and 8.1.0 of ONTAP can run in one of two modes; 7-mode or C-mode.
- NTP Software QFS for NAS, NetApp Edition requires the Cluster mode NetApp Filer to run Data ONTAP version 8.2 or later.

If the QFS license key supports NFS, the managed Filer ONTAP version need to be 7.3 or newer. If QFS is running on Windows Server 2008 or newer, it is recommended to upgrade to ONTAP version 7.3.3 or newer. If your Filer is running any version that is not supported, you must upgrade your operating system before you proceed; please refer to your NetApp documentation for instructions.

NTP Software QFS supports NFS with NetApp Filers. NTP Software QFS depends on the proper configuration of the Filer's user mapping file. Please refer to your NetApp documentation for instructions on how to set up the Filer user mapping file.

Data ONTAP versions 7.0.6 and 7.2.2 contain a number of fixes that address stability and memory issues related to fpolicy functionality in Data ONTAP. NetApp strongly recommends that customers using fpolicy move to one of these Data ONTAP versions or later (excluding version 7.1).

The Data ONTAP 7.1 release family is currently not supported by fpolicy.

For more information on NetApp Filers, consult NetApp Customer Support Bulletin CSB-0704-02: Fpolicy Update for Data ONTAP.

Adding Your Filer to the NTP Software QFS Policy Hierarchy

Next, you need to add your Filer to the collection of servers being managed by NTP Software QFS.

1. Run NTP Software QFS Admin by clicking Start > Programs > NTP Software QFS for NAS > NTP Software QFS for NAS Admin.

2. Right-click My Site and select New > Filer.

3. You will be prompted to enter a name. The name you enter here must match the name of your NetApp Filer.

4. Now that you have added your Filer to the collection of servers recognized by NTP Software QFS, right-click the Filer you just added and select New > Quota File & Sentinel Application. Entries will appear under the Filer for Disk Quota and File Control policies.

5. Next, we need to associate the policies you will create here with a Filer. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed NTP Software QFS.

6. Right-click Quota & File Sentinel under that entry and select Properties to open the NTP Software QFS Configuration screen.

7. Click the **NetApp Connector** tab.

8. Click the **Add** button.

9. Enter the name of your Filer and click **OK**.

10. Click **OK** in the **NTP Software QFS Configuration** screen.

Preparing the EMC CIFS Server

Refer to this section only if you have one or more EMC CIFS Servers attached to your environment. If you do not have EMC CIFS Servers, you should not apply the instructions specified in this section.

Preparing the NTP Software QFS Windows Machine

Perform the the following steps to prepare the Windows machine to host NTP Software QFS:

1. Before installing NTP Software QFS, you have to make sure that Celerra Event Enabler (CEE) version 4.5.2.3 or later is appropriately installed and configured in your environment. Contact EMC for further information on this configuration. CEE versions from 6.0.0 until 6.0.3 are not supported. If you will install CEE version 6.x then it must be 6.0.4 or higher. If you need to manage VNX (8.1.3+), then you must use CEE version 6.6 or higher.

2. NTP Software QFS requires the EMC Celerra to run DART version 5.6.49.3 or later. If your Celerra is not running version 5.6.49.3 or later, you must upgrade your operating system before you proceed; refer to your EMC documentation for instructions.

3. After installing the Celerra Event Enabler on the NTP Software QFS machine, you need to specify the software with which the CEE will register. To do this, set NTP for the following key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\EMC\Celerra Event
   Enabler\CEPP\CQM\Configuration\EndPoint
   ```

   If you installed CEE version 6.0.4 or higher, then the registry value will be:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\CQM\Configuratio
   n\EndPoint
   ```

NOTES:

- If NTP Software QFS is installed on an environment that has 'NTP Software FA with Proxy Service' installed, the registry value named "ProxyServer" in the registry key named "HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\ECS" on the QFS machine must be set to the machine name on which 'FA with Proxy Service' is installed. This allows NTP Software QFS and ‘FA with Proxy Service’ to work properly on the same environment.

Important: Two special permissions; “Event Notification ByPass” and “Virus Checking”, should be assigned to the EMC connector service account on the PDM that hosts the managed CIFS Server

EMC Connector service is registering with only one EMC Proxy service. That EMC Proxy service registers with all EMC CAVA services that are registered with all managed EMC NAS devices.

The connector registry key in EMC edition is:

HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\ECS

The following registry value needs to be configured under the connector registry key:

> **ProxyServer**: a string value, that should contain either the NetBiosName or the Fully Qualified Domain Name (FQDN) of the NAS Proxy service machine. If this value is empty or doesn't exist, the local machine name is used.

Important:

- There is flexibility to manage specific NAS device(s) through NAS Proxy service different than the one defined in the connector registry key.
- The user can create the **ProxyServer** registry value under the NAS device registry key, to allow the Connector service to manage this specific NAS device by a specific NAS Proxy service. This registry value is not created under the NAS device registry key by default.
- The user needs to create it manually, only if, he/she needs to manage this specific NAS device by a specific NAS Proxy service.
- If this value is empty or doesn't exist, the value under the connector registry key will be used, if it is also empty or doesn't exist, the local machine name is used.

The NAS device registry key in EMC edition is:

HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\ECS\ConnectedCelerras\<Device name>

The following are the two registry values that the user might set in the registry per the NAS device, in addition to the **ProxyServer** registry value described above.

I. **ApplicationPriority**: the NAS Proxy service orders registered applications based on priority. This registry value is a DWORD value that should contain the application priority according to which it will receive the requests from the registered NAS Proxy services, and its responses will be processed by those NAS Proxy services. The default value for this registry value is 4, and the minimum is 0 and the maximum is 100. If the user sets this registry value to any value outside this range, QFS will set it automatically to the default value.

II. **ConnectionMaintPeriodInSec:** A DWORD value that should contain the interval in seconds for the Connector service to check the status of its connection with the registered NAS Proxy services that is managing this NAS device. The default value for this registry value is 4 seconds, and the minimum is 1 second and the maximum is 300 seconds (5 minutes). If the user sets this registry value to any value outside this range, QFS will set it automatically to the default value**.**

4. The following are the two registry values that the user might set in the registry per the NAS device for the NAS Proxy service.

   HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\NasProxy\ConnectedNasDevices\<Device name>

- **ConnectionMaintPeriodInSec:** A DWORD value that should contain the interval in seconds for the NAS proxy service to maintain the connection with the registered NAS device. The default value for this registry value is 4 seconds, and the minimum is 1 second and the maximum is 300 seconds (5 minutes). If the user sets this registry value to any value outside this range, the NAS Proxy service will set it automatically to the default value.
- **NoReqProcThreads**: A DWORD value that should contain the number of requests processing threads for the managed NAS Device. The user can change this value according to the load on each of their managed NAS devices i.e. Increase the number of threads for busy NAS devices and decrease it for non-busy NAS devices. The default value for this registry value is 20 threads, and the minimum is 1 thread and the maximum is 50. If the user sets this registry value to any value outside this range, the NAS Proxy service will set it automatically to the default value.

NOTES:

1. Changing the **NoReqProcThreads** registry value requires restarting the NAS Proxy service, so as the change takes effect.
2. In EMC edition, there are no updates related to the EMC CAVA service registry key/values. Each CAVA service should indicate its proxy server (which could be remote or local) using the **endpoint** registry value.
3. If the proxy server is local, the **endpoint** registry value should have the word 'ntp', otherwise the **endpoint** registry value should have the word 'ntp@*ProxyServerFQDN*' , i.e if the proxy service is installed on a machine named 'DevTeam.NTP.com' and it is not the local machine on which the EMC CAVA service is installed, then the **endpoint** registry value on the EMC CAVA service machine should be 'ntp@DevTeam.NTP.com'.

Preparing the EMC CIFS Server for NTP Software QFS Management

For any CIFS Server that will be managed by NTP Software QFS, once the server is started and has mounted its root filesystem, go to the .etc directory and create the cepp.conf file (if it does not exist). You have to edit this file to include your CEPP pool description.

NOTE: The cepp.conf file must contain at least one line defining the pool of CEPP servers. If the line is too long, you can add \ at the end of each line:

```
pool name=<poolname> servers=<IP addr1>|<IP addr2>|... \
preevents=<event1>|<event2>|....\
postevents=<event3>|<event4>|.. \
posterrevents=<event5>|<event6>|... \
option=ignore or denied \
reqtimeout=<time out in ms> \ retrytimeout=<time out in
ms>
```

Kindly note:

- Each event can include one or more (or all) of the following events:
    - OpenFileNoAccess
    - OpenFileRead
    - OpenFileWrite
    - CreateFile
    - CreateDir
    - DeleteFile
    - DeleteDir
    - CloseModified
    - CloseUnmodified
    - RenameFile
    - RenameDir

  - SetAclFile
  - SetAclDir

- Postevents and posterevents are not supported in NTP Software QFS. We recommend turning them off to improve performance. Dropping those two fields from the CEPP will stop the Celerra Control Station from generating events of those types from that Data Mover.
- At least one event, one pool, and one server per pool must be defined.

Recommended timeout values:

- The recommended value for reqtimeout is 5000.
- The recommended value for retrytimeout is 750.

Perform the following steps to edit the cepp.conf file:

1. Log on to the celerra control station as su.
   a. Type `mount server_2:/ /mnt2` to mount the root filesystem. (Create /mnt2 if it does not exist, and replace server_2 with your Physical Data Mover name if you are configuring a different Physical Data Mover.)
   b. Type cd /mnt2/.etc and look for the file cepp.conf. Create the file if it does not exist.
   c. Use vi to edit the cepp.conf file. Edit the servers field to use the IP address of the machine running NTP Software QFS. The result should look something like this:

```
pool    name=cqm    servers=10.30.3.57    preevents=*
option=ignore reqtimeout=5000 retrytimeout=750
```

2. Type server_cepp server_2 –service -stop and press Enter.
3. Type server_cepp server_2 –service -start and press Enter.

> **NOTE:** Replace `server_2` with the name of the Physical Data Mover you want to configure.

These steps create the configuration that allows NTP Software QFS to register with and manage your CIFS Server. They must be completed before you try to configure NTP Software QFS.

Adding a CIFS Server to the NTP Software QFS Policy Hierarchy

Next, you need to add your EMC CIFS Server to the collection of servers being managed by NTP Software QFS.

1. Run NTP Software QFS Admin by clicking **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.

2. Right-click **My Site** and choose **New** > **Celerra**.

3. You will be prompted to enter a name. The name you enter here must match the name of your EMC CIFS Server.

4. Now that you have added your EMC CIFS Server to the collection of servers recognized by NTP Software QFS, right-click the EMC CIFS Server you just added and select **New** > **Quota** & **File Sentinel Application**.

   Entries will appear under the EMC CIFS Server for disk quota and file control policies.

5. Next, you need to associate the policies you will create here with an EMC CIFS Server. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed NTP Software QFS.

6. Right-click **Quota & File Sentinel** under that entry and select **Properties** to open the **NTP Software QFS Configuration** screen.

7. Click the **EMC Connector** tab.

8. Click the **Add** button.

9. Enter the needed information; name of your EMC CIFS Server, the control station IP, username, and password. At the end of the wizard, click **Finish**.

10. Click **OK** in the **NTP Software QFS Configuration** screen.

You are ready to move on and create some policies.

Preparing Hitachi NAS

Refer to this section only if you have Hitachi NASs attached to your environment. If you do not have Hitachi NASs, you should not apply the instructions specified in this section.

Preparing the Hitachi NAS for NTP Software QFS

Copyright © 2000-2015 NTP Software

Management

There is now one generic NAS proxy service handling both EMC and Hitachi editions. The registry configuration needs to be configured properly to manage the NAS devices correctly.

To prepare the Hitachi NAS server, the following must be taken into consideration:

1. For each EVS (virtual server) managed by NTP Software QFS, at least one CIFS server name must be created and must join the same domain as the QFS machine.

2. The logon account used to register with the Hitachi NAS (the account that will be assigned to the QFS connector service) needs to be a member of the Hitachi server's local group Backup Operators, which can be added from the Hitachi Server command-line interface (CLI) using the following command:

   ```
   localgroup add "Backup Operators" <FQDomainName\AccountName>
   ```

3. The File-Filtering feature must be enabled. To enable it, use the following command:

   ```
   fsm set allow-ntp-file-filtering true
   ```

4. Turn on File-Filtering after the Connector service is started. This can be done by running the following command on the Hitachi Server management CLI (it will start the notifications flow):

   ```
   file-filtering –on
   ```

   NOTE: The preceding step must be performed after NTP Software QFS is fully installed, so please follow up on the installation sections step by step, as explained in the Installation Guide, until you are advised to perform this step.

5. In the Hitachi connector registry key, enter the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\BCS

The following registry value needs to be configured under the connector registry key:

- **ProxyServer**: A string value that should contain either the NetBiosName or the Fully Qualified Domain Name (FQDN) of the NAS Proxy service machine. If it is empty or doesn't exist, the local machine name is used.

NOTES:

- There is flexibility to manage specific NAS device(s) through NAS Proxy service different than the one defined in the connector registry key.
- The user can create the **ProxyServer** registry value under the NAS device registry key, to allow the Connector service manage this specific NAS device by a specific NAS Proxy service.
- This registry value is not created under the NAS device registry key by default. The user needs to create it manually, only if, he/she needs to manage this specific NAS device by a specific NAS Proxy service.
- If this value is empty or doesn't exist, the value under the connector registry key will be used, if it is also empty or doesn't exist, the local machine name is used.

6. The NAS device registry key in Hitachi edition is:

HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\BCS\ConnectedTitans\<Device name>

NOTES

The following are the two registry values that the user might set in the registry per the NAS device, in addition to the **ProxyServer** registry value as described above.

I. **ApplicationPriority**: NAS Proxy service orders registered applications based on priority. This registry value is a DWORD value that should contain the application priority according to which it will receive the requests from the registered NAS Proxy services, and its responses will be processed by those NAS Proxy services. The default value for this registry value is 4, and the minimum is 0 and the maximum is 100. If the user sets this registry value to any value outside this range, QFS will set it automatically to the default value.

II. **ConnectionMaintPeriodInSec**: A DWORD value that should contain the interval in seconds for the Connector service to check the status of its connection with the registered NAS Proxy services that is managing this NAS

	device. The default value for this registry value is 4 seconds, and the minimum is 1 second and the maximum is 300 (5 minutes). If the user sets this registry value to any value outside this range, QFS will set it automatically to the default value.

Adding an EVS to the NTP Software QFS Policy Hierarchy

Next, you need to add your EVS to the collection of servers being managed by NTP Software QFS.

1. Run NTP Software QFS Admin by clicking **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.

2. Right-click My Site and choose **New** > **EVS**.

3. You will be prompted to enter a name. The name you enter here must match the name of your EVS.

4. Now that you have added your EVS to the collection of servers recognized by NTP Software QFS, right-click the EVS you just added and select **New** > **Quota & File Sentinel** Application.

   Entries will appear under the EVS for disk quota and file control policies.

5. Next, you need to associate the policies you will create here with an EVS. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed NTP Software QFS.

6. Right-click **Quota & File Sentinel** under that entry and select **Properties** to open the **NTP Software QFS Configuration** screen.

7. Click the **Hitachi Connector** tab.

8. Click the **Add** button.

9. Enter the name of your EVS.

10. Click **OK**.

11. Click **OK** in the **NTP Software QFS Configuration** screen.

Copyright © 2000-2015 NTP Software

NRT (Near Real Time) Devices

Unlike NAS devices in QFS editions, NRT devices do not send notifications to the connector service. User actions occur on files/directories on the NAS device. Instead of real-time processing of user actions, an NRT connector performs periodic scanning on the managed directories of the NAS device, to apply some operations and policy enforcement.

For example, a periodic scanning for a directory managed by Quota policy, finds that a managed user is over quota limit on that directory. In this case the QFS connector service applies deny-write security configurations on that directory for this user. This means the user will not be able to add more files to that managed directory, which is the same result of denying write operations in real-time devices when the user exceeds the quota limit.

The difference is that real-time devices such as Filers do not apply security configurations on the managed directory to enforce policies. Instead the Filer notifies the connector about the user action (when the user is trying to add a file, for example) and the connector processes that user action at real time and reply to the Filer telling it to deny this user action.

Since NRT devices are not real time, the user may still be able to write after they exceed the quota limit, until the next periodic scanning occurs. Periodic scanning can apply File Control Policies (FCPs) by either Delete or Quarantine files that match the policy criteria. Periodic scanning can be configured from a registry value named “PeriodicScanMode”, that is under the NRT Connector registry key:

“HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\NRT”

It represents 3 different modes of re-scan, which depend on the number of days that should elapse between each two successive re-scanning for all managed directories, as in the table below.

For more details of registry value, kindly check the table below:

Registry Key	Expected values	
PeriodicScanMode	0	No periodic scans, just the initial one (on start)
	1	In addition to initial one, run scan at midnight (if scanning isn't already running)
	2	In addition to initial one, run scan on Friday's midnight (if scanning isn't already running)

Preparing EMC Isilon

Refer to this section only if you have EMC Isilon devices attached to your environment. If you do not have EMC Isilon devices, you should not apply the instructions specified in this section.

Preparing the EMC Isilon for NTP Software QFS Management

To prepare the EMC Isilon, the following must be taken into consideration:

1. Each Isilon managed by NTP Software QFS must join the same domain as the QFS machine.

2. The logon account used to register with the EMC Isilon (the account that will be assigned to the QFS connector service) needs to be a member of the Isilon's local Administrators group.

Adding an Isilon to the NTP Software QFS Policy Hierarchy

Next, you need to add your Isilon to the collection of servers being managed by NTP Software QFS.

1. Run NTP Software QFS Admin by clicking **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.

2. Right-click **My Site** and choose **New** > **Isilon**.

3. You will be prompted to enter a name. The name you enter here must match the name of your Isilon.

4. Now that you have added your Isilon to the collection of servers recognized by NTP Software QFS, right-click the Isilon you just added and select **New** > **Quota & File Sentinel** Application.

   Entries will appear under the Isilon for disk quota, file control and file management policies.

5. Next, you need to associate the policies you will create here with an Isilon. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed NTP Software QFS.

6. Right-click **Quota & File Sentinel** under that entry and select **Properties** to open the **NTP Software QFS Configuration** screen.

7. Click the **NAS Connector** tab.

8. Click the **Add** button.

9. Enter the name of your Isilon.

10. Click **OK**.

11. Click **OK** in the **NTP Software QFS Configuratio**n screen.

Preparing Dell NAS

Refer to this section only if you have Dell NASs attached to your environment. If you do not have Dell NASs, you should not apply the instructions specified in this section.

Preparing the Dell NAS for NTP Software QFS Management

To prepare the Dell NAS, the following must be taken into consideration:

1. Each Dell NAS managed by NTP Software QFS must join the same domain as the QFS machine.

2. The logon account used to register with the Dell NAS (the account that will be assigned to the QFS connector service) needs to be a member of the Dell NAS's local Administrators group.

Adding a Dell NAS to the NTP Software QFS Policy Hierarchy

Next, you need to add your Dell NAS to the collection of servers being managed by NTP Software QFS.

1. Run NTP Software QFS Admin by clicking **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin**.

2. Right-click **My Site** and choose **New** > **Dell NAS**.

3. You will be prompted to enter a name. The name you enter here must match the name of your Dell NAS.

4. Now that you have added your Dell NAS to the collection of servers recognized by NTP Software QFS, right-click the Dell NAS you just added and select **New** > **Quota & File Sentinel** Application.

   Entries will appear under the Dell NAS for disk quota, file control and file management policies.

5. Next, you need to associate the policies you will create here with a Dell NAS. In the NTP Software Smart Policy Manager hierarchy view (the left pane), click the plus sign (+) adjacent to the name of the Windows-based server on which you installed NTP Software QFS.

6. Right-click **Quota & File Sentinel** under that entry and select **Properties** to open the **NTP Software QFS Configuration** screen.

7. Click the **NAS Connector** tab.

8. Click the **Add** button.

9. Enter the name of your Dell NAS.

10. Click **OK**.

11. Click OK in the **NTP Software QFS Configuration** screen**.**

User Group Resolution

When a user makes a user action on a managed NAS device, the connector service sends this user SID to QFS service to start resolving its user-group membership from Active Directory. The QFS service works on resolving group membership recursively from Active Directory, by continuously contacting Active Directory to retrieve the groups to which the current account belongs, in Depth first strategy, to get the whole 'Member Of' information in a complete manner. After the service finishes the resolution of the received user SID, it starts sending all of these groups to the connector service. The connector service then caches this user SID with its group membership information for better performance, and maintenance is done periodically for this cached information.

Group Group Resolution

In QFS service, the resolution procedure is extended to cache the group-group membership information after making user-group resolution for any user SID. A periodic maintenance is done concurrently on this cached information. This caching will enhance performance of user-group resolution mentioned above, because retrieving group membership from Active Directory will be done only once for each group on the 1st user action done by a user member of this group (either direct or indirect member) and it will be cached and maintained periodically, so any later resolution of group membership for the same group will be retrieved in no time from cache instead of retrieving it from Active Directory. At service shutdown, the QFS service will save the cached group-group information in a file named **'GrpGrpCache.dat'** in the installation directory.

Group Group Resolution Configuration

The group-group resolution cache is to be configurable by some registry values. The following registry values will be added under the following QFS service registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\NTPSoftware\Quota Sentinel Service

i. **GrpGrpCacheRefreshMinutes**: To configure the time period in minutes, according to which the cached resolution information is considered out-dated and needs to be updated again from Active Directory. The default value for this registry value is 30 Minutes, and the minimum is 5 minutes and the maximum is 10080 minutes (one week), inclusive. If the user sets this registry value to any value outside this range, QFS will set it automatically to the default value.

ii. **GrpGrpCacheExpireDays**: To configure the time period in days, according to which the resolution information is considered not used and needs to be deleted. The default value for this registry value is 20 days and the minimum is 10 and the maximum is 150 days (five months), inclusive. If the user sets this registry value to any value outside this range, QFS will set it automatically to the default value.

NAS Device Registeration Status

The user can check the status of each managed NAS device displayed under its "Quota & File Sentinel" tree node. There are three different statuses with specific icons for each managed NAS device; **Unknown**, **Managed**, and **Unmanaged**. The icon of the status node changes according to the NAS device status as shown below:

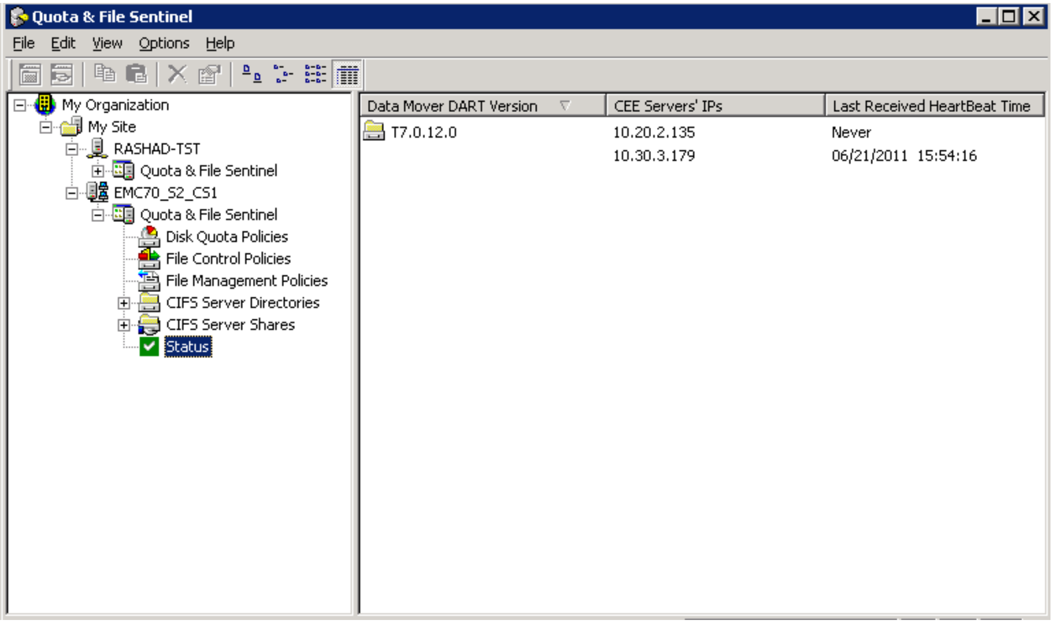
Icon	**Status**	**Case**
?	Unknown	At QFS Admin startup or when there is any failure in retrieving the status.
✓	Managed	When managed.
✗	Unmanaged	When unmanaged.

When the tree node of the NAS device status is selected, the right-hand list view displays different information about the NAS device depending on the connection status:

If the status is "**Managed**" the installed operating system on that NAS device will be displayed.

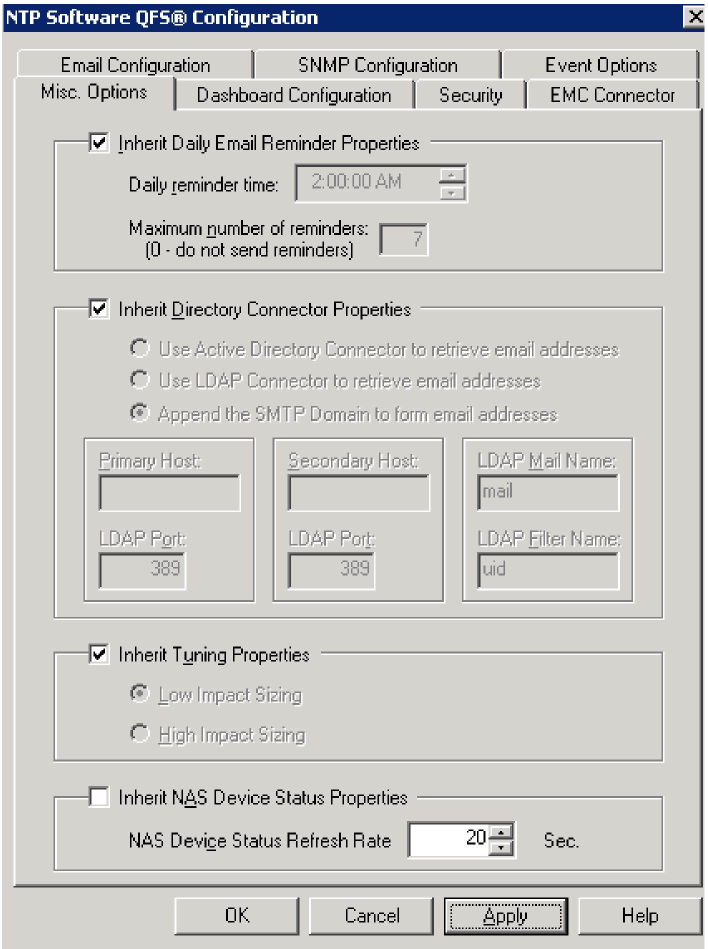
If the status is "**Unmanaged**", the reason of connection failure to the NAS device will be displayed.

NOTE: In case of the **Managed** status, the same is applied for EMC and Hitachi Editions, taking into consideration the name of the column i.e. 'Data Mover DART Version' in the case of the EMC Edition and 'EVS HOS Version' in the case of the Hitachi Edition.



Data Mover DART Version	CEE Servers' IPs	Last Received HeartBeat Time
T7.0.12.0	10.20.2.135	Never
	10.30.3.179	06/21/2011 15:54:16

At startup, the QFS Admin displays the status of all managed NAS devices as **'Unknown'** and the Filer ONTAP Version as 'Unknown'. Once the Admin retrieves the connection status of each managed NAS device, the data will be refreshed. The refresh rate is configurable in the "Misc. Options" tab in the **“Quota and File Sentinel” Properties** dialog box.



NTP Software QFS® Configuration

Email Configuration | SNMP Configuration | Event Options

Misc. Options | Dashboard Configuration | Security | EMC Connector

☑ Inherit Daily Email Reminder Properties

Daily reminder time: 2:00:00 AM

Maximum number of reminders: 7
(0 - do not send reminders)

☑ Inherit Directory Connector Properties

○ Use Active Directory Connector to retrieve email addresses
○ Use LDAP Connector to retrieve email addresses
● Append the SMTP Domain to form email addresses

Primary Host:
LDAP Port: 389

Secondary Host:
LDAP Port: 389

LDAP Mail Name: mail
LDAP Filter Name: uid

☑ Inherit Tuning Properties

● Low Impact Sizing
○ High Impact Sizing

□ Inherit NAS Device Status Properties

NAS Device Status Refresh Rate 20 Sec.

NOTES:

- The default refresh rate is 30 seconds while the minimum rate is 10 seconds and the maximum rate is 1 hour (3600 seconds).

- The refresh rate can be inherited from the global “Quota and File Sentinel” node in QFS hierarchy.

- IPs are written in the "cepp.conf" file of the host physical Data Mover, if their EMC CAVA services are connected with the control station. Any IP that is written in the "cepp.conf" file but doesn't contain CEE or its CEE is not connected with the control station will not be listed. The 2nd column displays the last HeartBeat time received by the managing connector service from the corresponding EMC CAVA service.

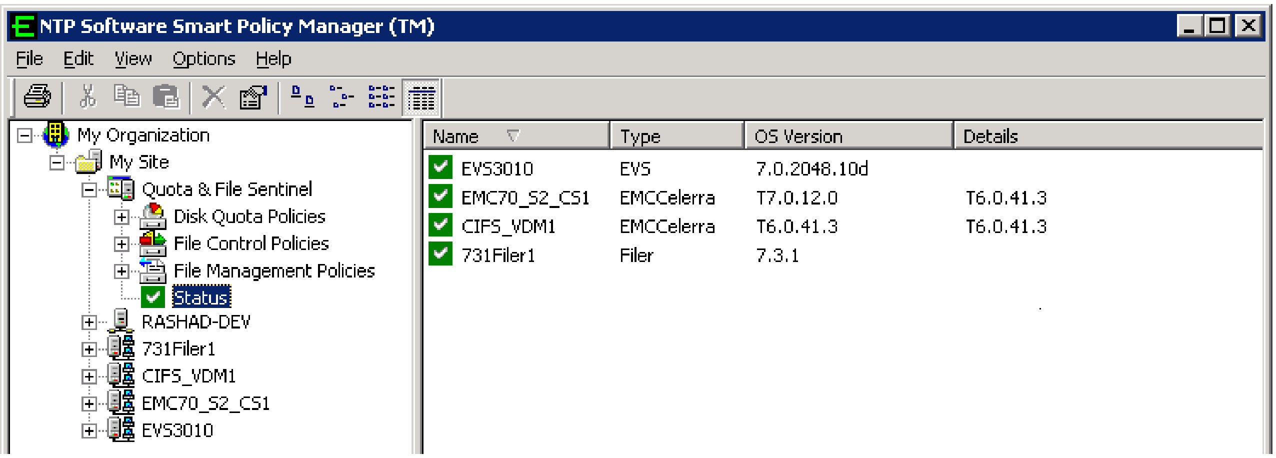
Checking the Container Status

The Container Status node summarizes the status of managed NAS devices under any container. It is displayed under the "Quota & File Sentinel" tree node of each container.

According to the status of the managed NAS device(s) under that container, it can be in one of the following states:

Icon	Status	Description
?	**Unknown**	This is the default status, which will be displayed at startup, and when the status of any managed NAS device under that container is **Unknown** and none of them is Unmanaged.
✓	**Managed**	This is displayed when the status of all managed NAS devices under that container are Managed.
✗	**Unmanaged**	This is displayed when the status of any managed NAS device under that container is Unmanaged.
⊘	**Not Applicable**	This is displayed when the container has no managed NAS device under it.

At startup, the QFS Admin displays the default status of the container, which is **Unknown**, until it retrieves the connection status of all managed NAS devices under it. Once the user selects the status node under any container, the connection status of all managed NAS devices or sub-containers under it is listed on the right with some information about these NAS devices or sub-containers.



Name	Type	OS Version	Details
✓ EVS3010	EVS	7.0.2048.10d	
✓ EMC70_S2_CS1	EMCCelerra	T7.0.12.0	T6.0.41.3
✓ CIFS_VDM1	EMCCelerra	T6.0.41.3	T6.0.41.3
✓ 731Filer1	Filer	7.3.1	

Copyright © 2000-2015 NTP Software

NOTES

- The icon of the Container Status node is set according to the highest status severity of its managed NAS devices or sub-containers. The status severities are as follows in descending order from the most to least severe: **Unmanaged** status, **Unknown** status, **Managed** status. If a container is empty, then its status will be displayed as **Not Applicable** and it will be ignored in calculating its parent container status.
- The Container status node is refreshed according to the statuses of the managed NAS devices. The refresh rate is configured from the '**Misc. Options**' tab.
- NRT NAS devices do not have a status node under its "Quota and File Sentinel" node, and as a consequence these devices will not be considered in computing the status of any container that contains them. NRT NAS devices will not be listed in the list of the managed NAS devices/sub-containers when their container status node is selected in the tree.
- In case of EMC Celerra NAS device, the status validation will check that at least one IP of the QFS connector machine IPs is present in the 'servers=' section of the cepp.conf file, on the host PDM of the managed CIFS server. If the QFS machine IP is missing, the status will be displayed as **Unmanaged**.

Diagnosing NAS Device Status

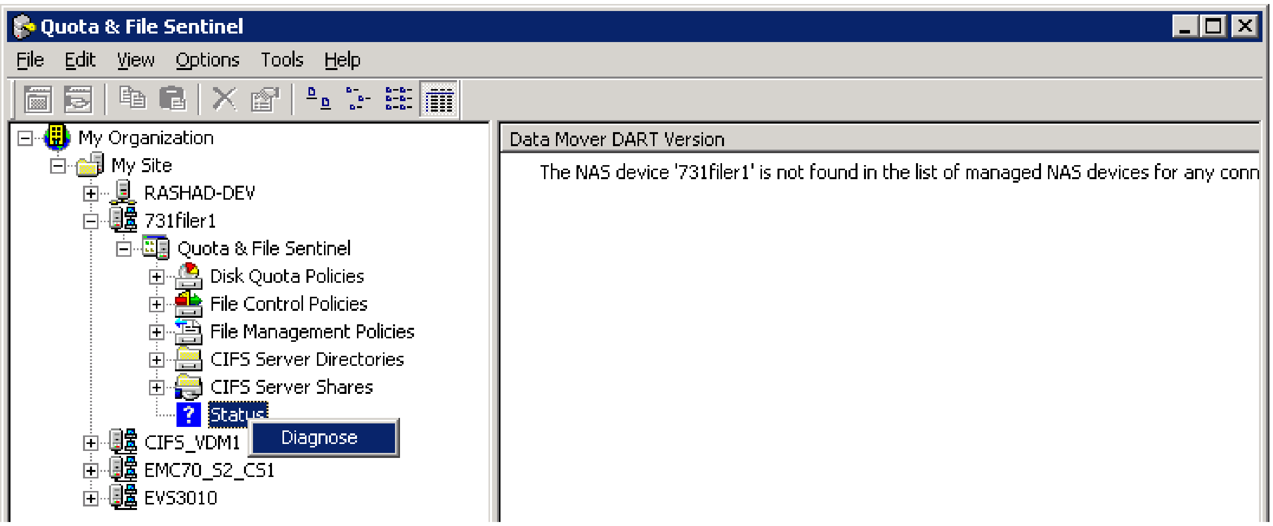
The user is enabled to diagnose a managed NAS device in case it is **Unmanaged**, **Unknown**, or even **Managed**. During the diagnosis process, the QFS Admin communicates with the QFS services and they should be up and running on the connector machine. QFS validates either QFS Service or Connector Service statuses depending on the diagnosis. If any service is down the diagnosis will not start.

NOTES:

- If there is a firewall controlling the QFS connector machine, then it should open the ports used by QFS services in order for QFS to work properly e.g. receiving user actions occur on the managed NAS device and respond to them, sending emails, popups, RPC calls between services… etc.
- If the QFS connector machine is controlled by firewall and any port is not opened, QFS will try to open those ports. If QFS failed to open the ports, the Firewall Settings validation test will be marked as failed.

To diagnose a NAS device status, perform the following steps:

1. Right-click the Status node in the tree, under any managed NAS device.
2. Select **Diagnose** menu item.



The NAS device '731filer1' is not found in the list of managed NAS devices for any conn

Copyright © 2000-2015 NTP Software

NOTES: The diagnosis process differs according to the NAS device type. The diagnosis has 2 forms based on the NAS device type:

- For NetApp Filer and Hitachi EVS: a progress dialogue appears to notify the user about the validation test that is currently in progress. If all validation tests succeed, a completion message is eventually displayed.
- For EMC Celerra CIFS Server: a sequence of dialogues is displayed, where each dialogue validate a certain aspect of EMC NAS device management requirements, and the user is allowed to move forward in the diagnose process or retry the current diagnosis step if failed, or even quit the whole diagnosis process.

Showing Advanced Configuration Parameters

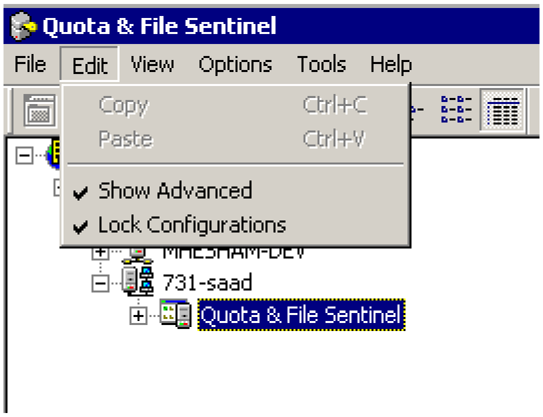
The Basic/Advanced configuration mode is a method of hiding/displaying more advanced configuration parameters from/to the user to prevent confusion and/or misconfiguration. All configuration parameters are categorized as either **Basic** or **Advanced**. By default, QFS Admin is configured to run in Basic mode when first installed. The intent is to not even let the user know that the advanced parameters exist when in Basic mode.

NOTES:

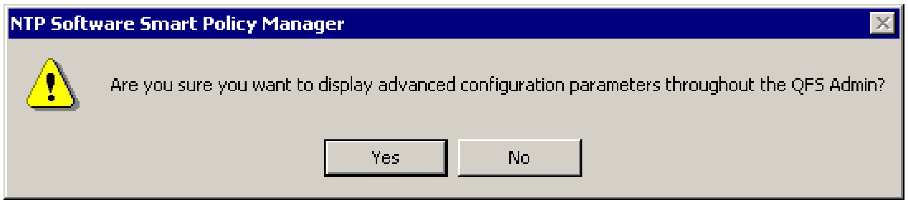
- The state of the Basic/Advanced mode will be stored in the QFS Admin machine registry.
- If the QFS Admin is closed and reopened, the Basic/Advanced state will return to what it was before the Admin was closed.

To show advanced configuration parameters, perform the following steps:

1. From the **Edit** menu, select **Show Advanced**.



2. In the warning dialog box, click **Yes**.


NTP Software Smart Policy Manager

Are you sure you want to display advanced configuration parameters throughout the QFS Admin?

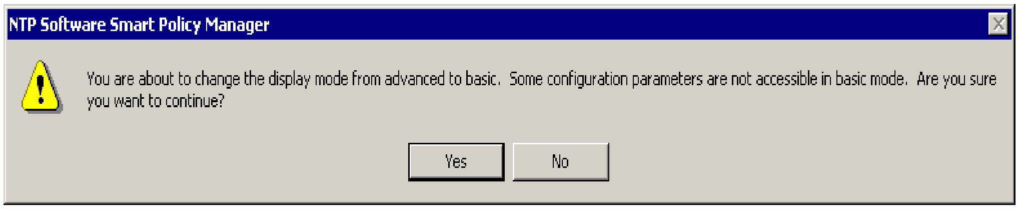
A check mark will appear next to the **Show Advanced** menu item and the Admin will show all configuration parameters (basic and advanced) in all controls and dialogues.

Copyright © 2000-2015 NTP Software

NOTE: To return to the Basic display mode, perform the following steps:

1. From the **Edit** menu, click the checked **Show Advanced** menu item.

2. In the warning dialog box, click **Yes**.



NTP Software Smart Policy Manager

You are about to change the display mode from advanced to basic. Some configuration parameters are not accessible in basic mode. Are you sure you want to continue?

.

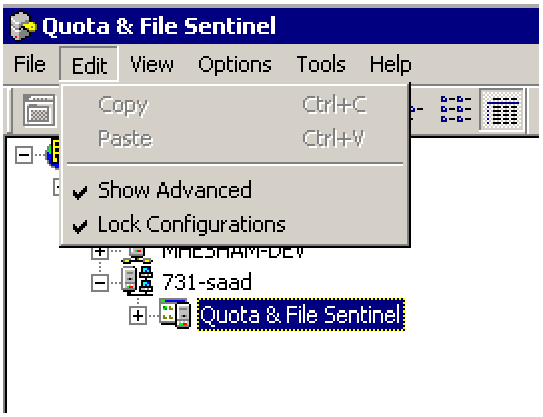
Locking Configuration Parameters

The user can set many QFS configuration parameters to be "read only". When in the locked state, designated parameters cannot be changed but are visible through the QFS Admin. This is typically accomplished by disabling the control that holds the configuration parameter. By default, QFS Admin is configured to run in unlocked state when first installed.

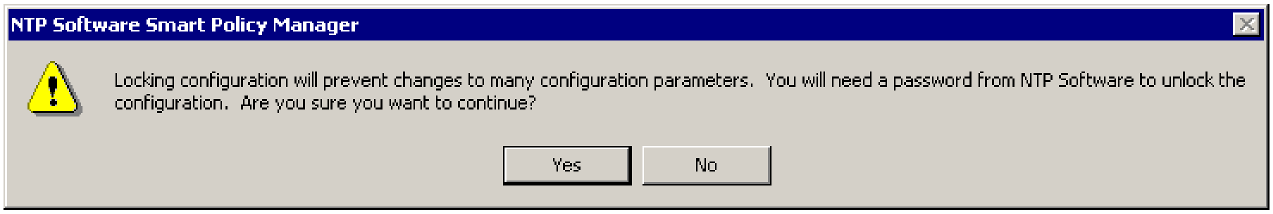
NOTE: The locking does not prevent users from changing configuration through the CLI or a script.

To lock configurations, perform the following steps:

1. From the **Edit** menu, select **Lock Configurations**.



2. In the warning dialog box, click **Yes**.



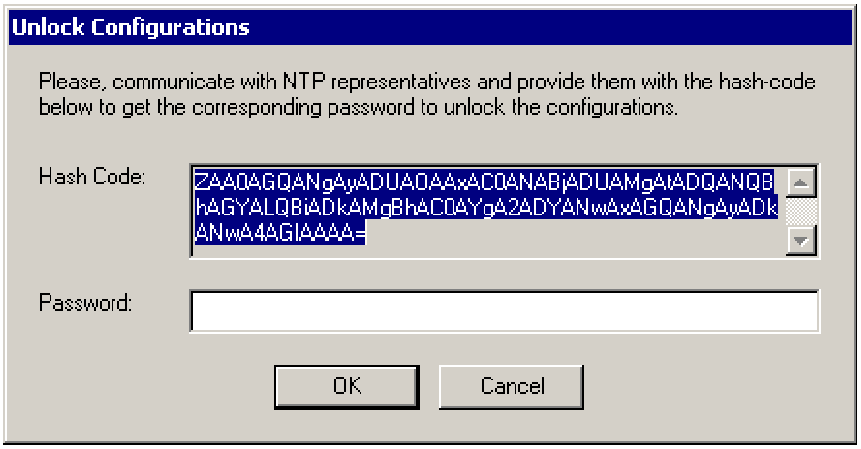
NTP Software Smart Policy Manager

Locking configuration will prevent changes to many configuration parameters. You will need a password from NTP Software to unlock the configuration. Are you sure you want to continue?

A check mark will appear next to the **Lock Configurations** menu item and the Admin will enter the locked state.

NOTE: To return to the unlocked mode, perform the following steps:

1. From the **Edit** menu, click the marked **Lock Configurations** menu item.
2. In the **Unlock Configuration** dialog box, enter the password provided to you from NTP Software and click **OK**.



Unlock Configurations

Please, communicate with NTP representatives and provide them with the hash-code below to get the corresponding password to unlock the configurations.

Hash Code: ZAA0AGQANgAyADUAOAAxAC0ANABjADUAMgAtADQANQBhAGYALQBiADkAMgBhAC0AYgA2ADYANwAxAGQANgAyADkANwA4AGIAAAA=

Password:

Important: The locked state will be stored in EASE so all installed QFS Admins will have access to the same state. When locked, all Admins will be locked. When unlocked, all Admins will be unlocked.

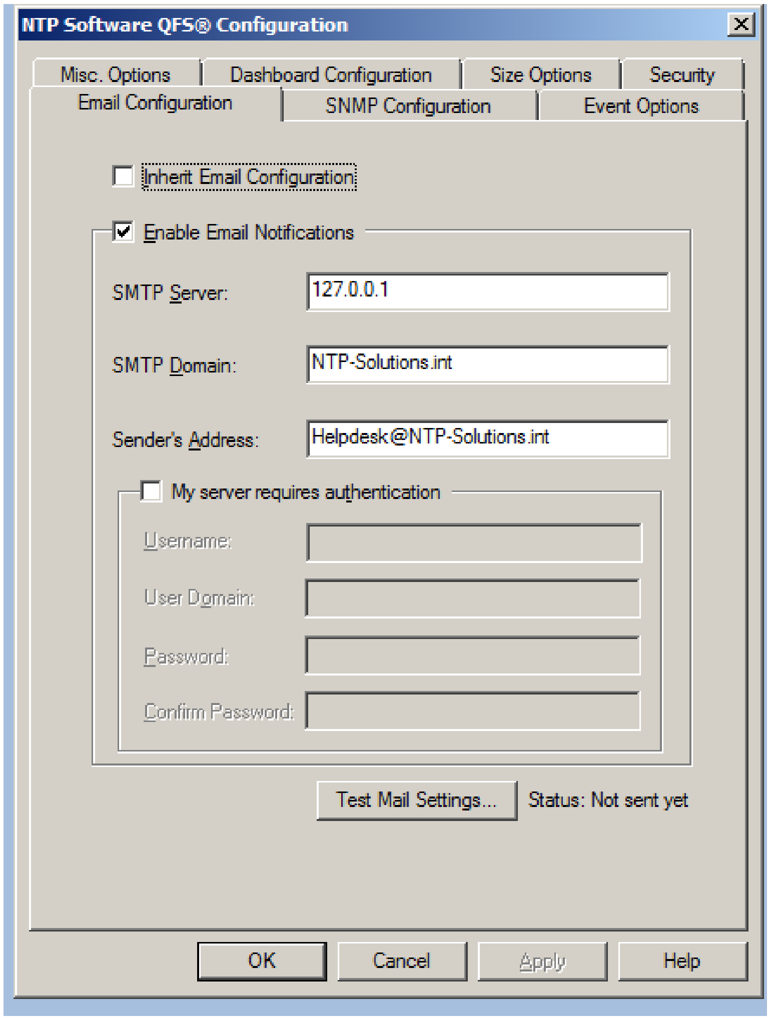
Relating Basic/Advanced Mode with Locking state

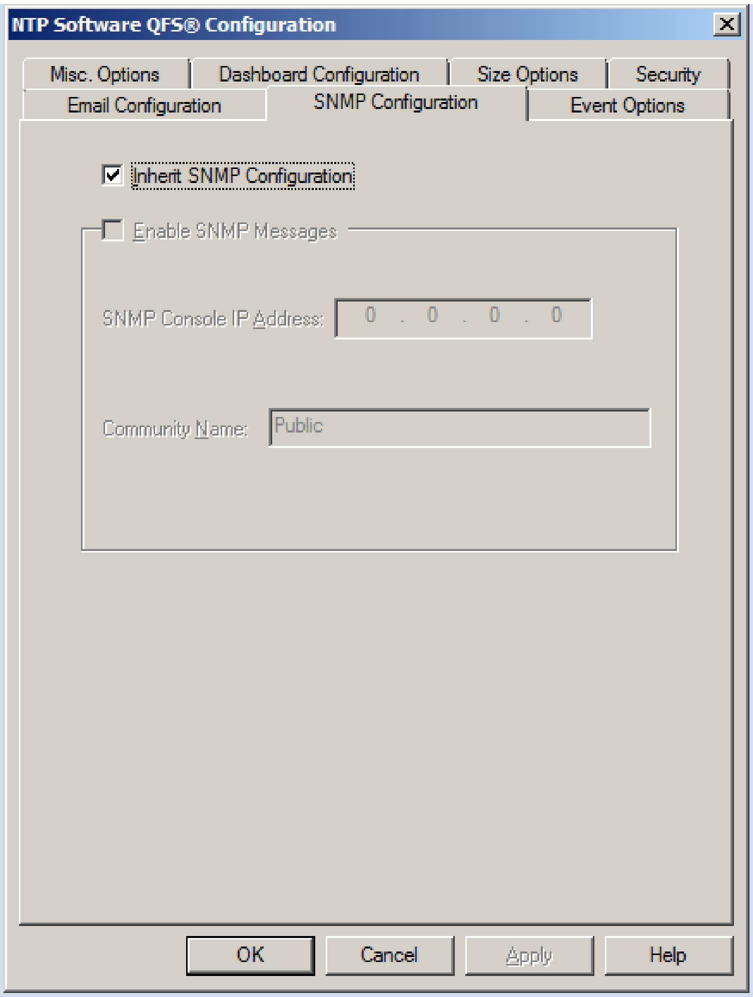
The **Basic/Advanced** and **Lock** features are related to each other, because they both change how the user sees the UI and deals with it. Simply, the Basic/Advanced feature is responsible for showing/hiding some controls, while the Lock feature is responsible for disabling/enabling some controls. Both features can target the same control, and they will not overlap or conflict with each other.

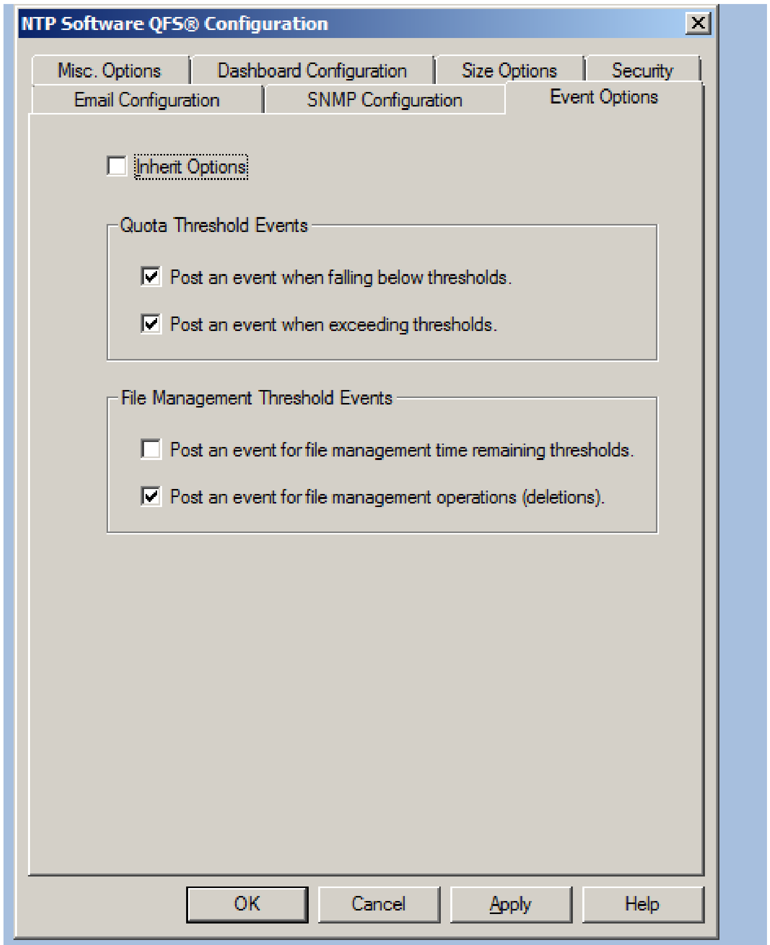
The rule of treating a configuration parameter grouping control in the same way as the configuration parameter itself will apply for any configuration parameter, if and only if the grouping control contains only one configuration parameter. If the grouping control contains more than one configuration parameter, then the grouping control will be disabled if all grouped controls are disabled, and it will be hidden if all grouped controls should be hidden.

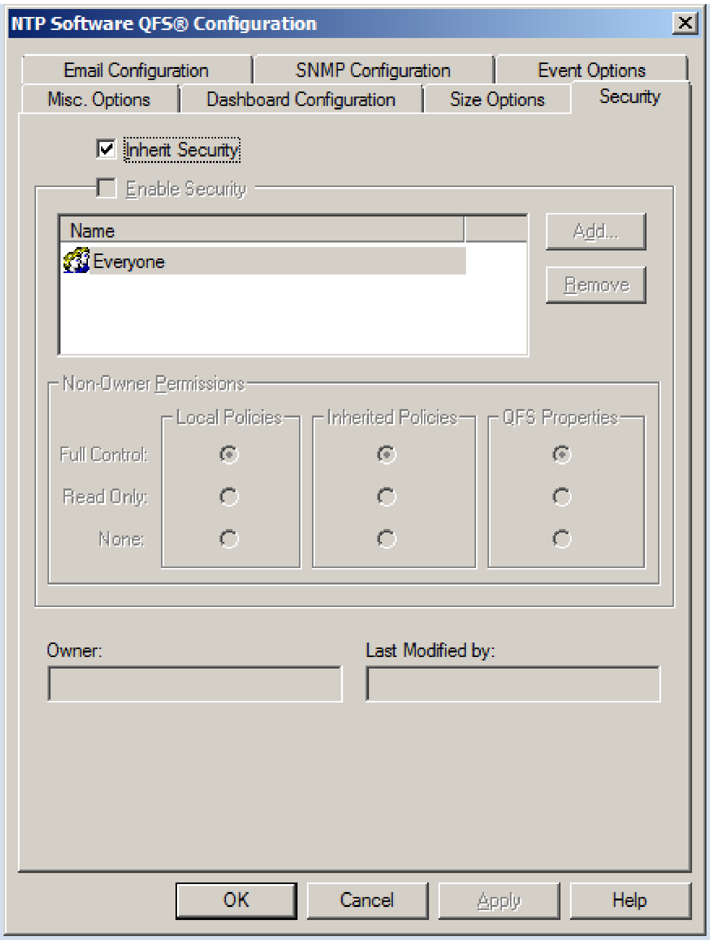
A tab-page can be categorized as a whole to be Basic or Advanced, and governed by the Lock feature or not. A tab-page categorized as Advanced will be completely hidden and will not appear in the tab-sheet. A tab-page governed by the Lock feature will have all its controls disabled if QFS Admin is in locked state, and enabled otherwise. If a subset of a tab-page controls is explicitly categorized to be Basic or Advanced or governed by the Lock feature, then the other - non-categorized - configuration parameters are implied to be Basic parameters, or NOT governed by the Lock feature (i.e. not lockable).

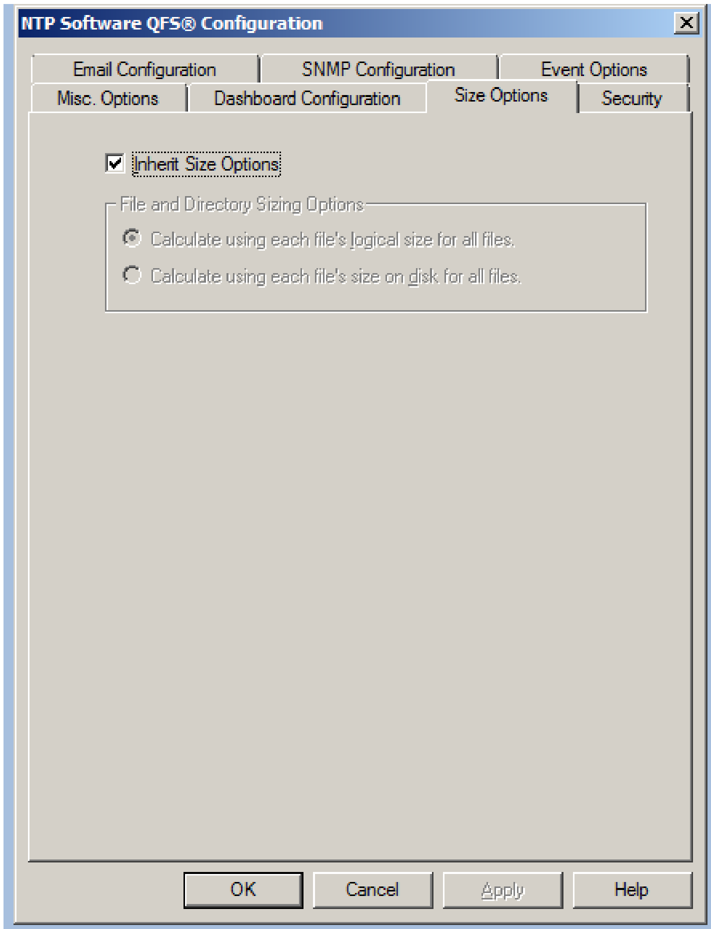
Following is a screen-shot for each tab-page containing a set of configuration parameters, with a categorization for each of its controls (i.e. configuration parameters) as Basic or Advanced, and which control is governed by the Lock feature (i.e. lockable).

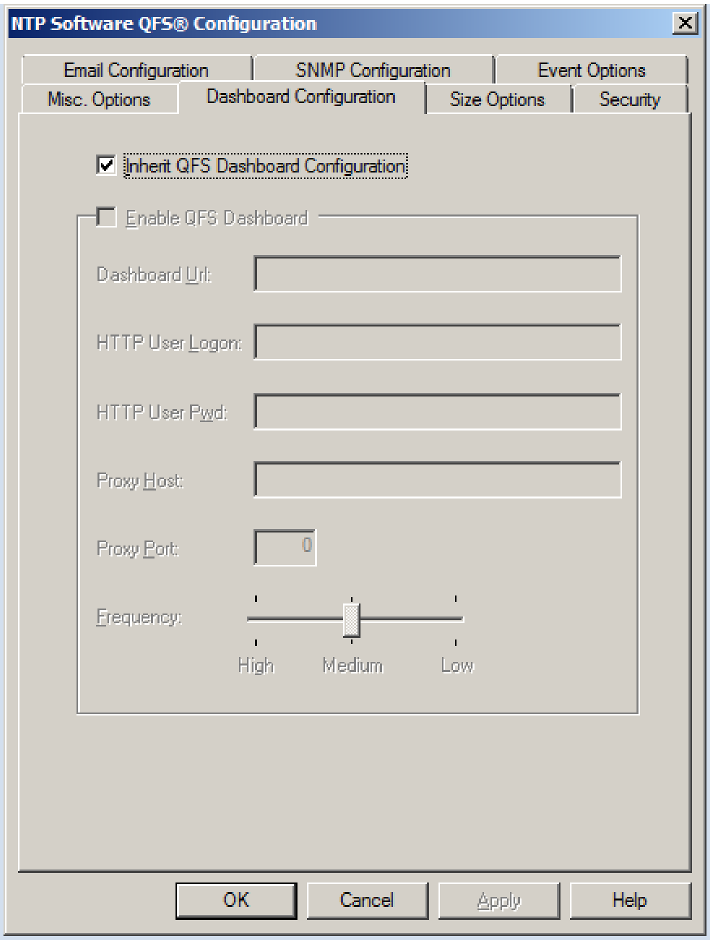
Tab-page	Screenshot	Control Categorization
Email Configuration	 NTP Software QFS® Configuration Misc. Options Dashboard Configuration Size Options Security Email Configuration SNMP Configuration Event Options ☐ Inherit Email Configuration ☑ Enable Email Notifications SMTP Server: 127.0.0.1 SMTP Domain: NTP-Solutions.int Sender's Address: Helpdesk@NTP-Solutions.int ☐ My server requires authentication Username: User Domain: Password: Confirm Password: Status: Not sent yet Test Mail Settings... OK Cancel Apply Help	Basic/Lockable

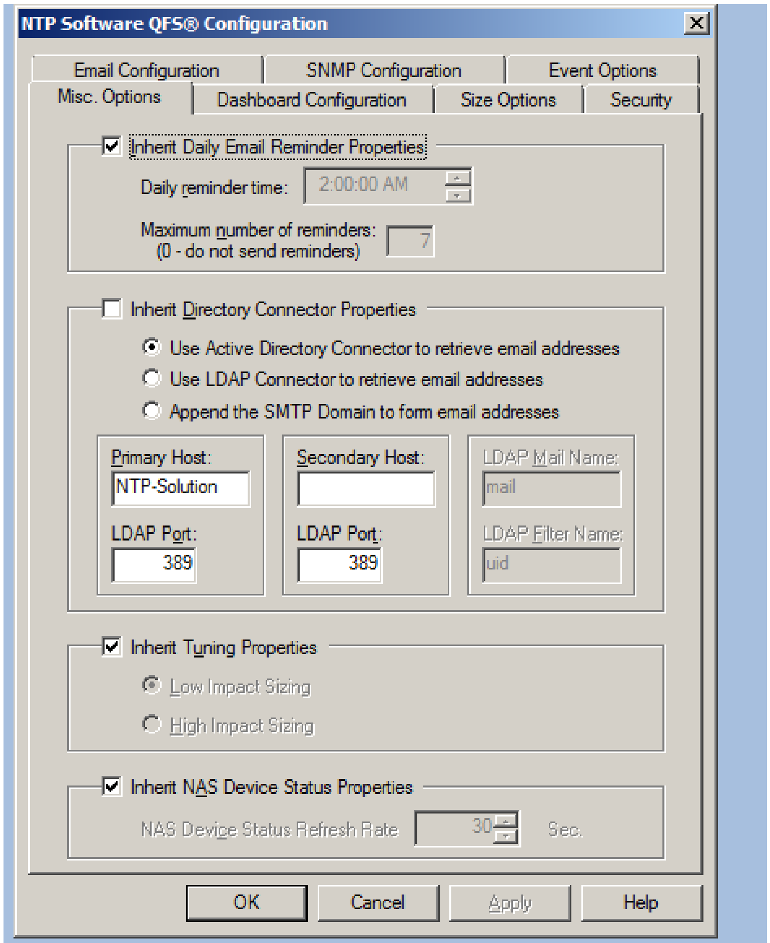
Tab-page	Screenshot	Control Categorization
SNMP Configuration	 NTP Software QFS® Configuration Misc. Options Dashboard Configuration Size Options Security Email Configuration SNMP Configuration Event Options OK Cancel Apply Help ☑ Inherit SNMP Configuration □ Enable SNMP Messages SNMP Console IP Address: 0 . 0 . 0 . 0 Community Name: Public	Advanced/Lockable

Tab-page	Screenshot	Control Categorization
Event Options	 NTP Software QFS® Configuration Misc. Options Dashboard Configuration Size Options Security Email Configuration SNMP Configuration Event Options OK Cancel Apply Help ☐ Inherit Options Quota Threshold Events ☑ Post an event when falling below thresholds. ☑ Post an event when exceeding thresholds. File Management Threshold Events ☐ Post an event for file management time remaining thresholds. ☑ Post an event for file management operations (deletions).	Advanced/Lockable

Tab-page	Screenshot	Control Categorization
Security	 NTP Software QFS® Configuration Email Configuration SNMP Configuration Event Options Misc. Options Dashboard Configuration Size Options Security Add... Remove OK Cancel Apply Help ☑ Inherit Security □ Enable Security Name: Everyone Non-Owner Permissions Local Policies: ● Full Control: ○ Read Only: ○ None: Inherited Policies: ● Full Control: ○ Read Only: ○ None: QFS Properties: ● Full Control: ○ Read Only: ○ None: Owner: Last Modified by:	Advanced/Lockable

Tab-page	Screenshot	Control Categorization
Size Options	 NTP Software QFS® Configuration ☑ Inherit Size Options File and Directory Sizing Options ● Calculate using each file's logical size for all files. ○ Calculate using each file's size on disk for all files. Email Configuration SNMP Configuration Event Options Misc. Options Dashboard Configuration Size Options Security OK Cancel Apply Help	Advanced/Lockable

Tab-page	Screenshot	Control Categorization
Dashboard Configuration	 NTP Software QFS® Configuration Email Configuration SNMP Configuration Event Options Misc. Options Dashboard Configuration Size Options Security ☑ Inherit QFS Dashboard Configuration ☐ Enable QFS Dashboard Dashboard Url: HTTP User Logon: HTTP User Pwd: Proxy Host: Proxy Port: 0 Frequency: Medium High Medium Low OK Cancel Apply Help	Advanced/Lockable

Tab-page	Screenshot	Control Categorization
Misc. Options	 .	Advanced/Lockable

NTP Software QFS® Configuration

☑ Inherit Daily Email Reminder Properties

Daily reminder time: 2:00:00 AM

Maximum number of reminders: 7
(0 - do not send reminders)

□ Inherit Directory Connector Properties

● Use Active Directory Connector to retrieve email addresses

○ Use LDAP Connector to retrieve email addresses

○ Append the SMTP Domain to form email addresses

Primary Host: NTP-Solution

LDAP Port: 389

Secondary Host:

LDAP Port: 389

LDAP Mail Name: mail

LDAP Filter Name: uid

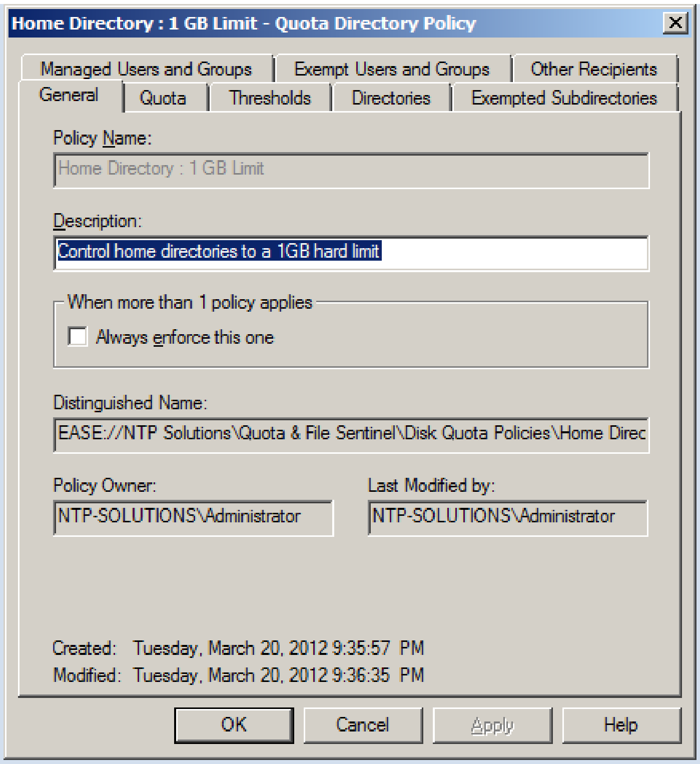
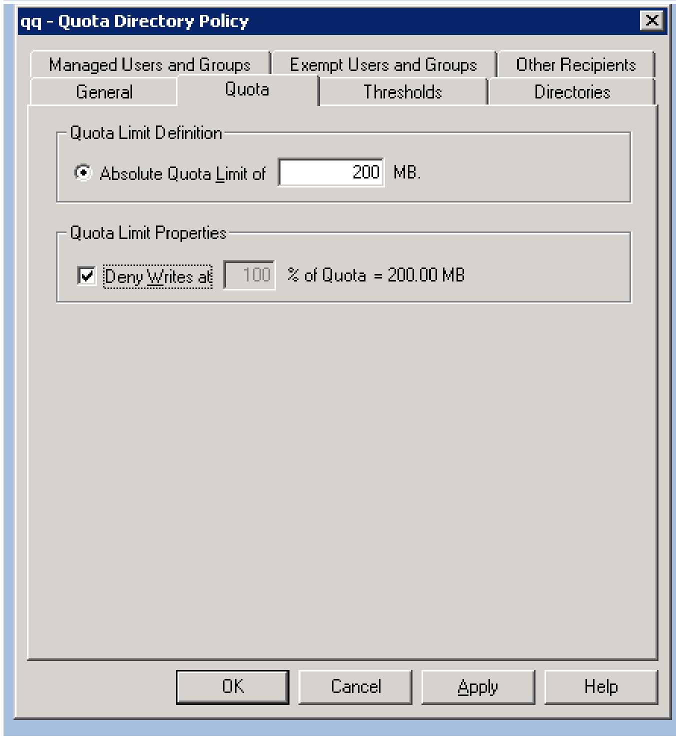
☑ Inherit Tuning Properties

● Low Impact Sizing

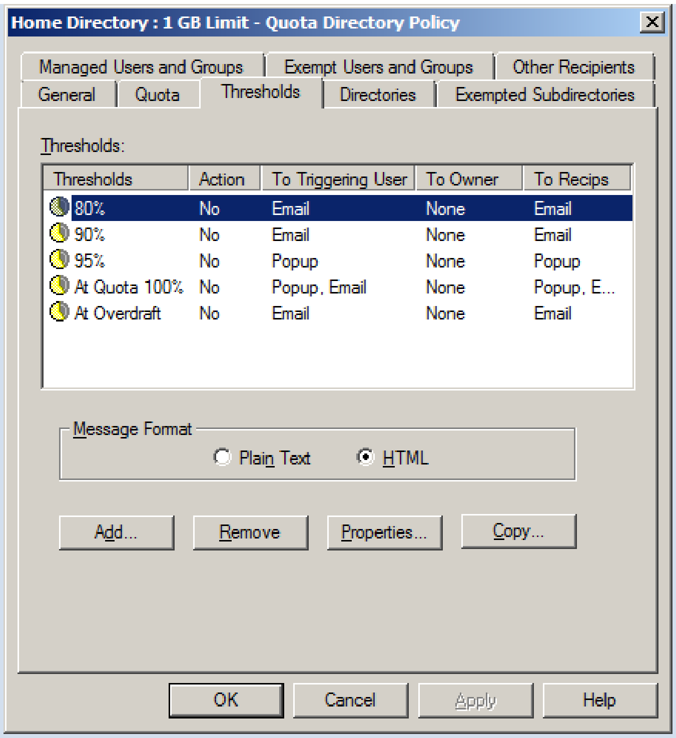
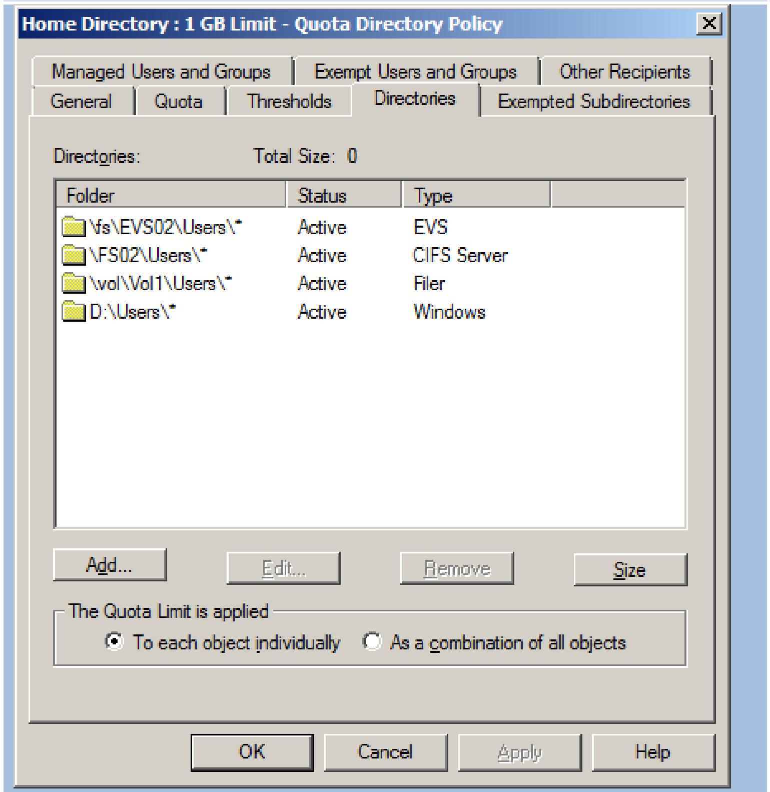
○ High Impact Sizing

☑ Inherit NAS Device Status Properties

NAS Device Status Refresh Rate 30 Sec.

Tab-page	Screenshot	Control Categorization
Disk Quota Policy : General	 Home Directory : 1 GB Limit - Quota Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Quota Thresholds Directories Exempted Subdirectories Policy Name: Home Directory : 1 GB Limit Description: Control home directories to a 1GB hard limit When more than 1 policy applies ☐ Always enforce this one Distinguished Name: EASE://NTP Solutions\Quota & File Sentinel\Disk Quota Policies\Home Direc Policy Owner: NTP-SOLUTIONS\Administrator Last Modified by: NTP-SOLUTIONS\Administrator Created: Tuesday, March 20, 2012 9:35:57 PM Modified: Tuesday, March 20, 2012 9:36:35 PM 	"Always enforce this one": Advanced/Lockable
Disk Quota Policy: Quota	 qq - Quota Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Quota Thresholds Directories Quota Limit Definition ● Absolute Quota Limit of 200 MB. Quota Limit Properties ☑ Deny Writes at 100 % of Quota = 200.00 MB OK Cancel Apply Help	In Basic mode. The Quota tab-page has 2 exceptional behaviors, and they are as follows: The __% of Quota is disabled in Basic and enabled in Advanced mode. Which means that on creating a new Disk Quota Policy in Basic mode, the user only has the option to set a soft quota (i.e. keep Deny Writes un-checked) or set a hard limit fixed to 100% of Quota - which is the default percentage.

Copyright © 2000-2015 NTP Software

Tab-page	Screenshot	Control Categorization
Disk Quota Policy: Thresholds		Nothing changes.
Disk Quota Policy: Directories		Quota limit is applied: Advanced/Lockable

Home Directory : 1 GB Limit - Quota Directory Policy

Tabs: Managed Users and Groups | Exempt Users and Groups | Other Recipients | General | Quota | Thresholds | Directories | Exempted Subdirectories

Thresholds:

Thresholds	Action	To Triggering User	To Owner	To Recips
80%	No	Email	None	Email
90%	No	Email	None	Email
95%	No	Popup	None	Popup
At Quota 100%	No	Popup, Email	None	Popup, E...
At Overdraft	No	Email	None	Email

Message Format: ○ Plain Text ● HTML

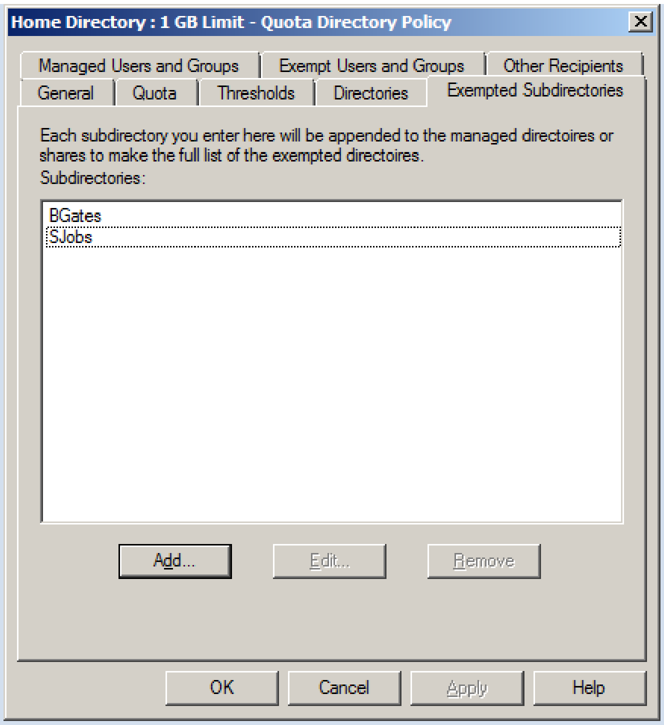
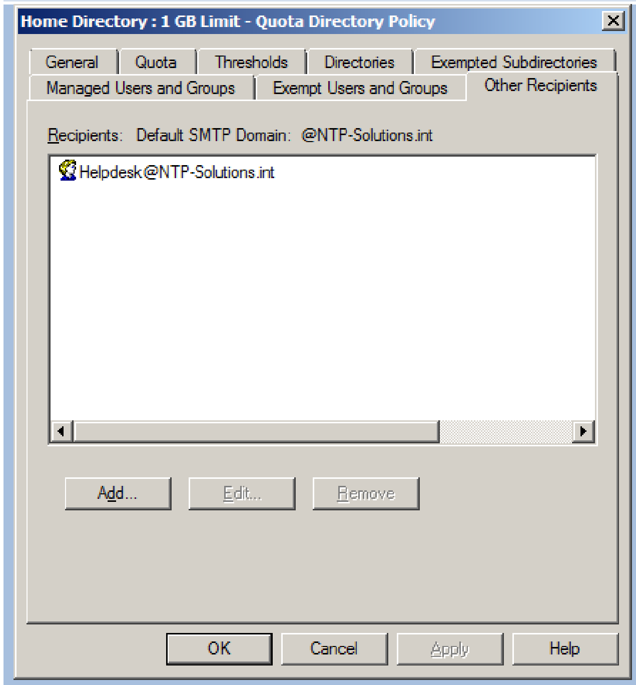
Home Directory : 1 GB Limit - Quota Directory Policy

Tabs: Managed Users and Groups | Exempt Users and Groups | Other Recipients | General | Quota | Thresholds | Directories | Exempted Subdirectories

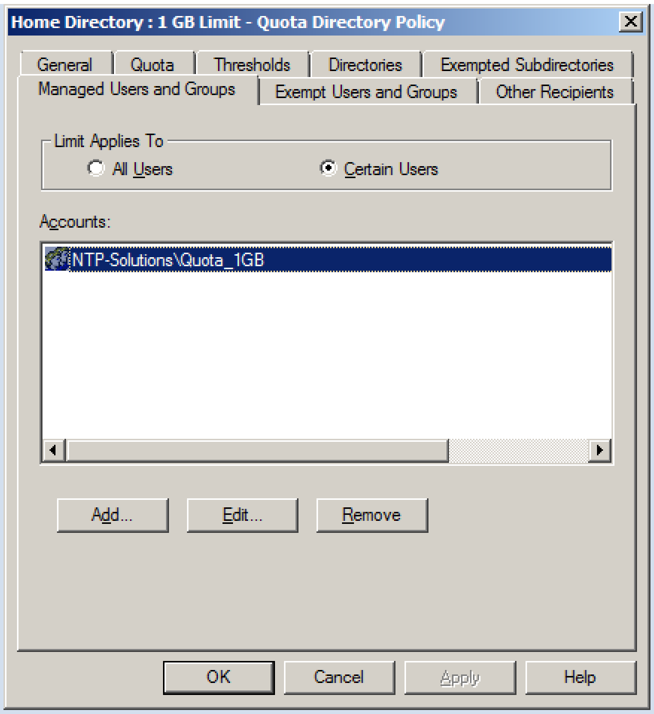
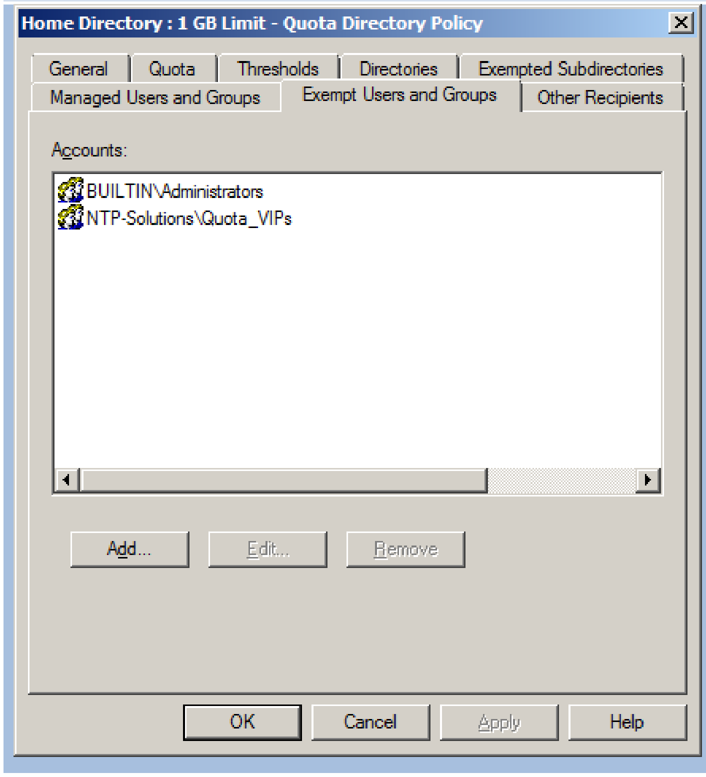
Directories: Total Size: 0

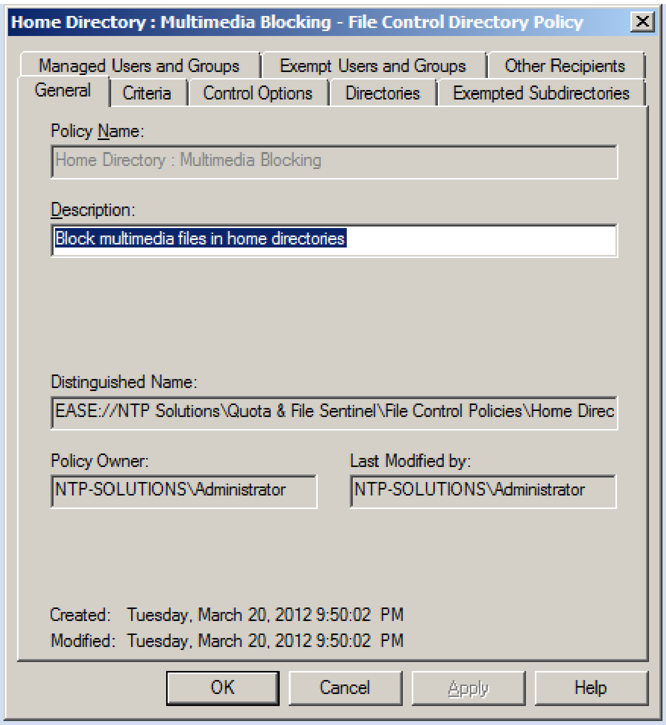
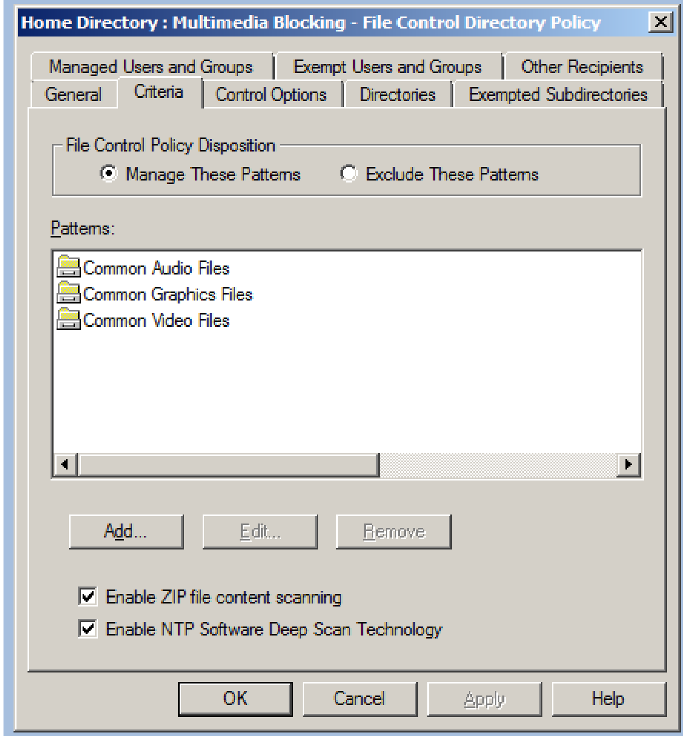
Folder	Status	Type
\fs\EVS02\Users\*	Active	EVS
\FS02\Users\*	Active	CIFS Server
\vol\Vol1\Users\*	Active	Filer
D:\Users\*	Active	Windows

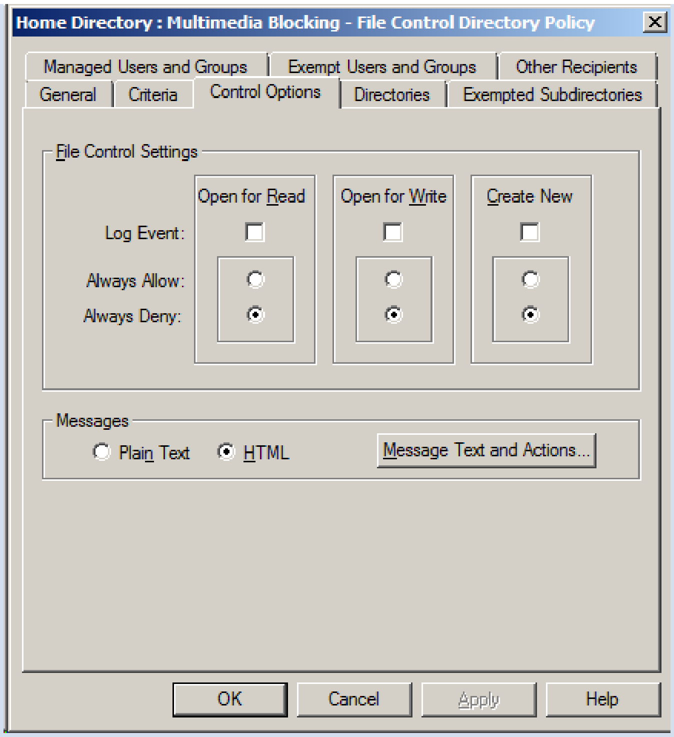
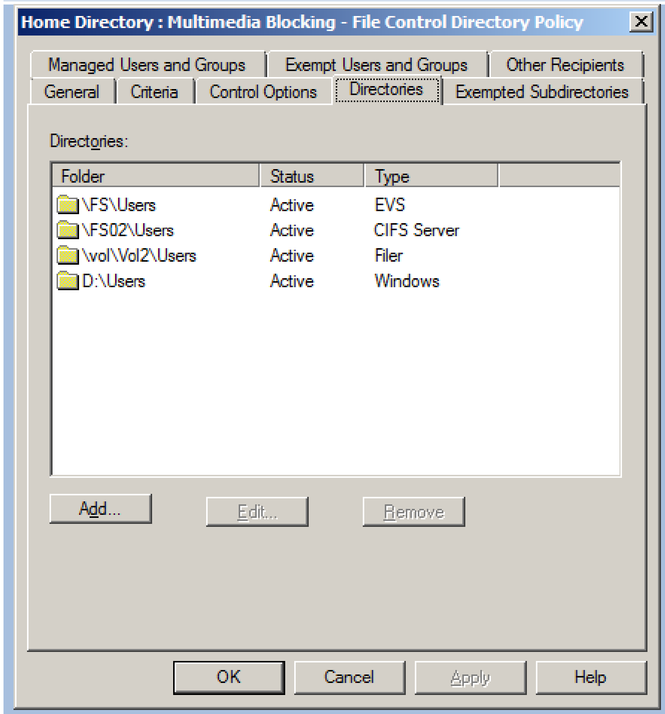
The Quota Limit is applied: ● To each object individually ○ As a combination of all objects

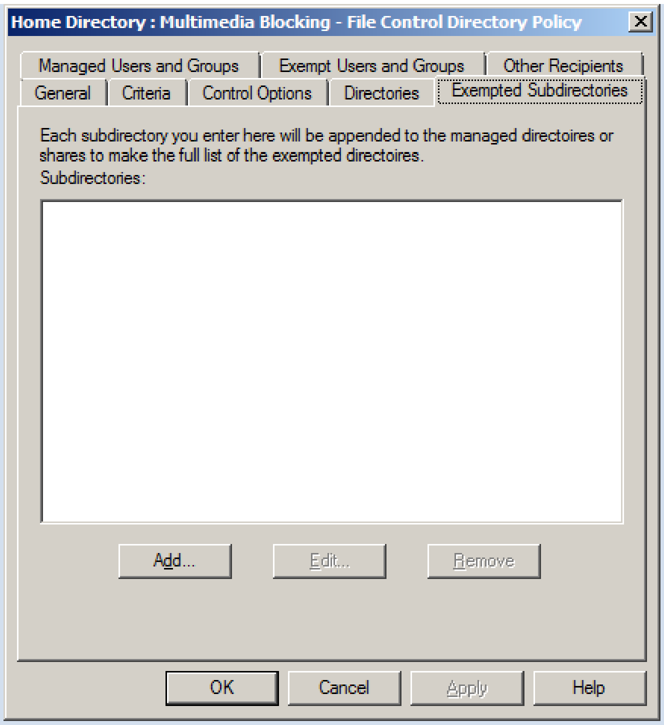
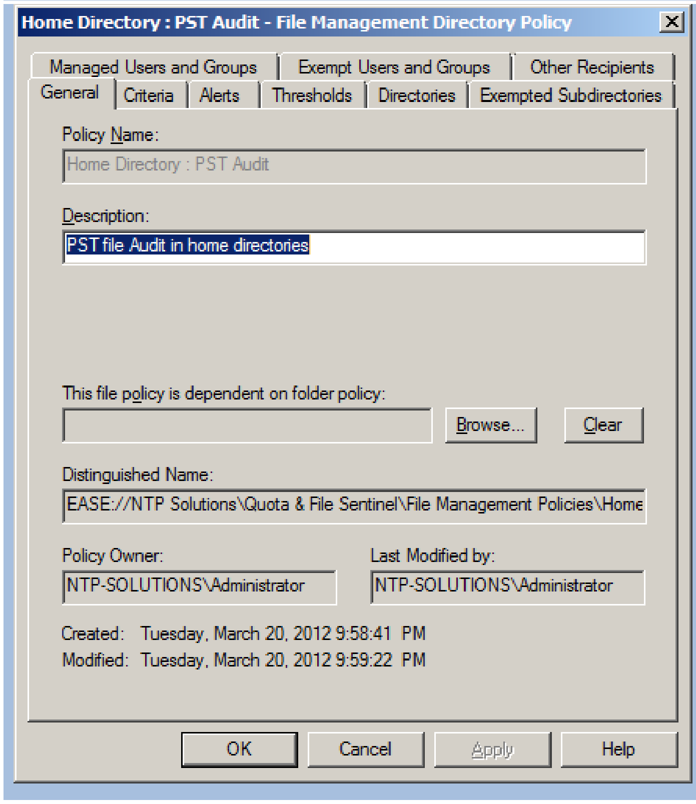
Tab-page	Screenshot	Control Categorization
Disk Quota Policy: Exempted Subdirectories	 Home Directory : 1 GB Limit - Quota Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Quota Thresholds Directories Exempted Subdirectories Add... Edit... Remove OK Cancel Apply Help Each subdirectory you enter here will be appended to the managed directoires or shares to make the full list of the exempted directoires. Subdirectories: BGates SJobs	Advanced/Lockable
Disk Quota Policy: Other Recipients	 Home Directory : 1 GB Limit - Quota Directory Policy General Quota Thresholds Directories Exempted Subdirectories Managed Users and Groups Exempt Users and Groups Other Recipients Add... Edit... Remove OK Cancel Apply Help Recipients: Default SMTP Domain: @NTP-Solutions.int Helpdesk@NTP-Solutions.int	Basic/Lockable

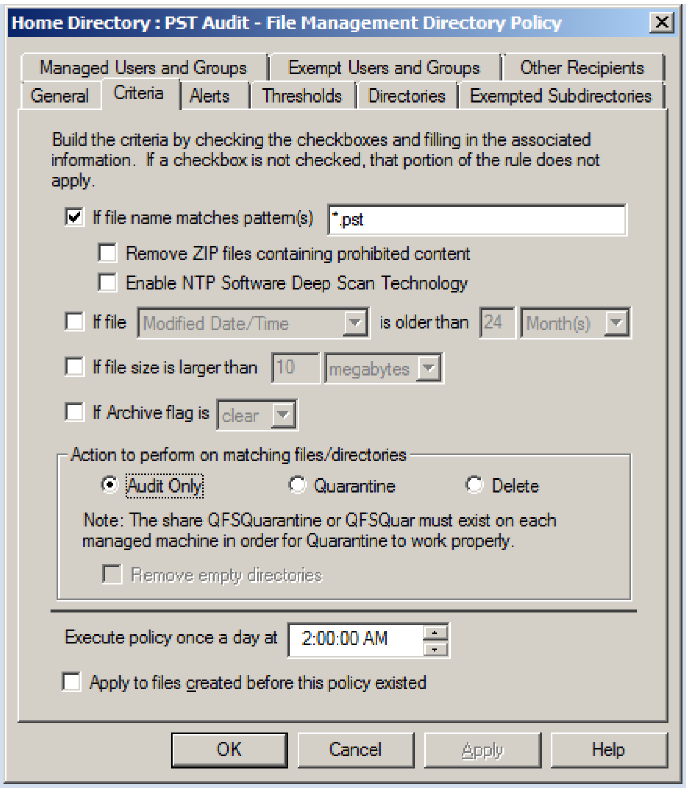
Copyright © 2000-2015 NTP Software

Tab-page	Screenshot	Control Categorization
Disk Quota Policy: Managed Users and Groups	 Home Directory : 1 GB Limit - Quota Directory Policy Limit Applies To ○ All Users ● Certain Users Accounts: NTP-Solutions\Quota_1GB General Quota Thresholds Directories Exempted Subdirectories Managed Users and Groups Exempt Users and Groups Other Recipients Add... Edit... Remove OK Cancel Apply Help	Basic/Lockable
Disk Quota Policy: Exempted Users and Groups	 Home Directory : 1 GB Limit - Quota Directory Policy Accounts: BUILTIN\Administrators NTP-Solutions\Quota_VIPs General Quota Thresholds Directories Exempted Subdirectories Managed Users and Groups Exempt Users and Groups Other Recipients Add... Edit... Remove OK Cancel Apply Help	Basic/Lockable

Tab-page	Screenshot	Control Categorization
File Control Policy: General	 Home Directory : Multimedia Blocking - File Control Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Control Options Directories Exempted Subdirectories Policy Name: Home Directory : Multimedia Blocking Description: Block multimedia files in home directories Distinguished Name: EASE://NTP Solutions\Quota & File Sentinel\File Control Policies\Home Direc Policy Owner: NTP-SOLUTIONS\Administrator Last Modified by: NTP-SOLUTIONS\Administrator Created: Tuesday, March 20, 2012 9:50:02 PM Modified: Tuesday, March 20, 2012 9:50:02 PM 	Nothing changes.
File Control Policy: Criteria	 Home Directory : Multimedia Blocking - File Control Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Control Options Directories Exempted Subdirectories File Control Policy Disposition ● Manage These Patterns ○ Exclude These Patterns Patterns: Common Audio Files Common Graphics Files Common Video Files Add... Edit... Remove ☑ Enable ZIP file content scanning ☑ Enable NTP Software Deep Scan Technology OK Cancel Apply Help	Zip Scan: Advanced/Lockable; unchecked is default Deep Scan: Advanced/Lockable; unchecked is default Disposition: Advanced/Lockable; Manage is default

Tab-page	Screenshot	Control Categorization
File Control Policy: Criteria	 Home Directory : Multimedia Blocking - File Control Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Control Options Directories Exempted Subdirectories OK Cancel Apply Help File Control Settings Open for Read / Open for Write / Create New Log Event: □ □ □ Always Allow: ○ ○ ○ Always Deny: ● ● ● Messages ○ Plain Text ● HTML Message Text and Actions...	Basic/Lockable
File Control Policy: Directories	 Home Directory : Multimedia Blocking - File Control Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Control Options Directories Exempted Subdirectories Add... Edit... Remove OK Cancel Apply Help Directories: Folder / Status / Type \FS\Users / Active / EVS \FS02\Users / Active / CIFS Server \vol\Vol2\Users / Active / Filer D:\Users / Active / Windows	Nothing changes.

Tab-page	Screenshot	Control Categorization
File Control Policy: Exempted Subdirectories	 Home Directory : Multimedia Blocking - File Control Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Control Options Directories Exempted Subdirectories Each subdirectory you enter here will be appended to the managed directoires or shares to make the full list of the exempted directoires. Subdirectories: Add... Edit... Remove OK Cancel Apply Help	Basic/Lockable File Control Policy: Managed Users and Groups tab-page: Basic/Lockable. File Control Policy: Exempt Users and Groups tab-page: Basic/Lockable File Control Policy: Other Recipients tab-page: Basic/Lockable
File Management Policy: General	 Home Directory : PST Audit - File Management Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Alerts Thresholds Directories Exempted Subdirectories Policy Name: Home Directory : PST Audit Description: PST file Audit in home directories This file policy is dependent on folder policy: Distinguished Name: EASE://NTP Solutions\Quota & File Sentinel\File Management Policies\Home Policy Owner: NTP-SOLUTIONS\Administrator Last Modified by: NTP-SOLUTIONS\Administrator Created: Tuesday, March 20, 2012 9:58:41 PM Modified: Tuesday, March 20, 2012 9:59:22 PM 	This file policy is dependent on the folder policy: Advanced/Lockable

Tab-page	Screenshot	Control Categorization
File Management Policy: Criteria		Deep Scan & Zip Scan: Advanced/Lockable Delete Action option: Advanced/Lockable

Home Directory : PST Audit - File Management Directory Policy

Build the criteria by checking the checkboxes and filling in the associated information. If a checkbox is not checked, that portion of the rule does not apply.

☑ If file name matches pattern(s) *.pst

☐ Remove ZIP files containing prohibited content

☐ Enable NTP Software Deep Scan Technology

☐ If file Modified Date/Time is older than 24 Month(s)

☐ If file size is larger than 10 megabytes

☐ If Archive flag is clear

Action to perform on matching files/directories

● Audit Only ○ Quarantine ○ Delete

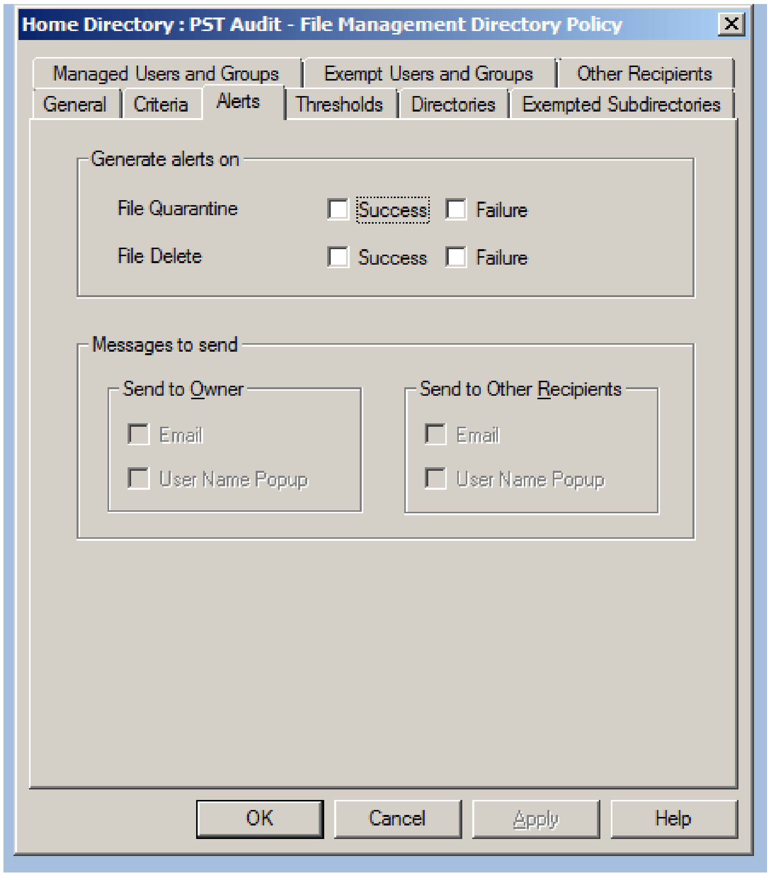
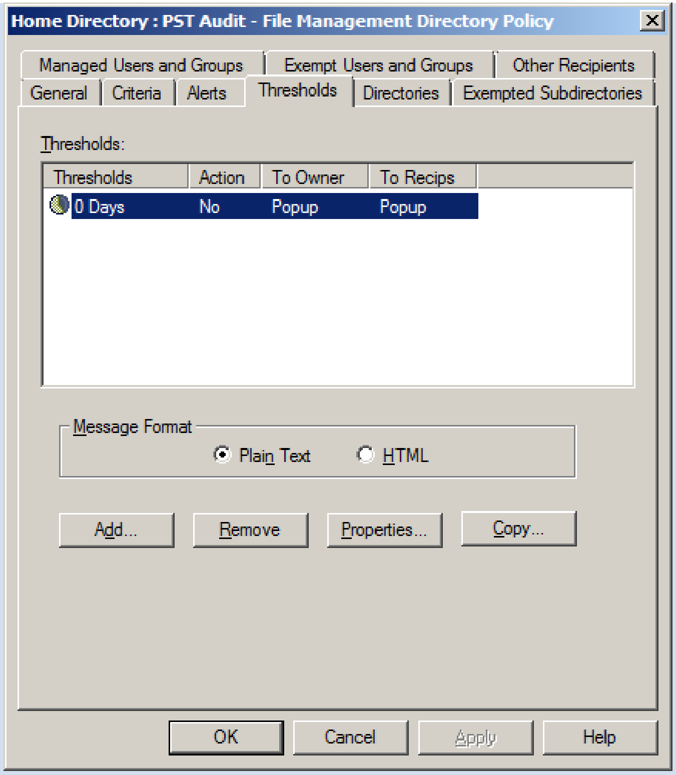
Note: The share QFSQuarantine or QFSQuar must exist on each managed machine in order for Quarantine to work properly.

☐ Remove empty directories

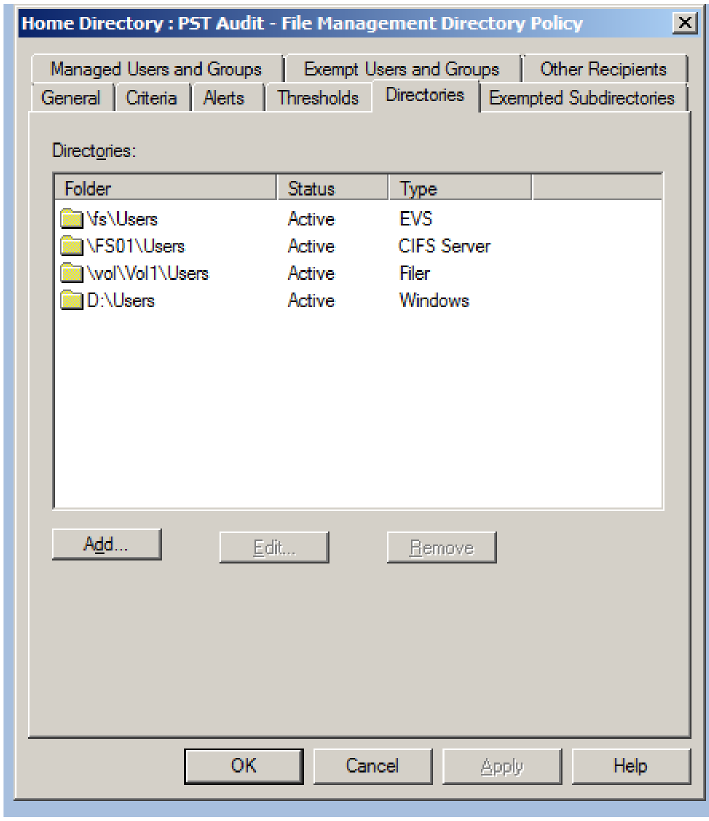
Execute policy once a day at 2:00:00 AM

☐ Apply to files created before this policy existed

Copyright © 2000-2015 NTP Software

Tab-page	Screenshot	Control Categorization
File Management Policy: Alerts	 Home Directory : PST Audit - File Management Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Alerts Thresholds Directories Exempted Subdirectories OK Cancel Apply Help Generate alerts on File Quarantine □ Success □ Failure File Delete □ Success □ Failure Messages to send Send to Owner □ Email □ User Name Popup Send to Other Recipients □ Email □ User Name Popup	Advanced/Lockable
File Management Policy: Thresholds	 Home Directory : PST Audit - File Management Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Alerts Thresholds Directories Exempted Subdirectories Add... Remove Properties... Copy... OK Cancel Apply Help Thresholds: Thresholds / Action / To Owner / To Recips 0 Days / No / Popup / Popup Message Format ● Plain Text ○ HTML	Advanced/Lockable

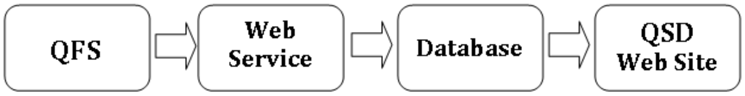
Copyright © 2000-2015 NTP Software

Tab-page	Screenshot	Control Categorization
File Management Policy: Directories	 Home Directory : PST Audit - File Management Directory Policy Managed Users and Groups Exempt Users and Groups Other Recipients General Criteria Alerts Thresholds Directories Exempted Subdirectories Directories: Folder / Status / Type \fs\Users / Active / EVS \FS01\Users / Active / CIFS Server \vol\Vol1\Users / Active / Filer D:\Users / Active / Windows Add... Edit... Remove OK Cancel Apply Help	Nothing changes. File Management Policy: Exempted Subdirectories: Basic/Lockable File Management Policy: Managed Users and Groups: Basic/Lockable File Management Policy: Exempt Users and Groups: Basic/Lockable File Management Policy: Other Recipients: Basic/Lockable

NTP Software QFS System Dashboard (QSD)

NTP Software QFS System Dashboard, referred to as QSD, is an add-on to NTP Software QFS. It is a web application that provides administrators with a high level of statistical information on their NTP Software QFS environment. This reporting tool is efficient for administrators because it provides critical information about the entire NTP Software QFS environment.

NOTE: QFS for Windows does not support QSD.



For QSD to report on your environment, you need to perform the following:

1. Run NTP Software QFS Admin by clicking Start > Programs > NTP Software QFS for NAS > NTP Software QFS for NAS Admin.

2. Right-click Quota & File Sentinel under the main Windows server.

3. Click **Properties** on the pop-up menu.

4. On the **Dashboard Configuration** tab, clear the box **Inherit QFS Dashboard Configuration** and check the box **Enable QFS Dashboard**.

5. Add the following information and then click **OK**:

Field	**Description**
Dashboard URL	Enter the following URL: http://webservername/QFSSystemDashboardWebService/QSDWS.asmx
HTTP user logon	Enter the HTTP username.
HTTP user password	Enter the HTTP password.
Proxy host	Enter the proxy host.
Proxy port	Enter the proxy port.
Frequency	This decides how frequently NTP Software QFS collects information to the web service, when the database is filled so as the website displays such data. This could be configured as follows: • High Frequency: 1 minute (NTP Software QFS will keep sending the collected data out of the users' transactions every 1 minute). • Medium Frequency: 15 minutes (NTP Software QFS will keep sending the collected data out of the users' transactions every 15 minutes). • Low Frequency: 30 minutes (NTP Software QFS will keep sending the collected data out of the users' transactions every 30 minutes).

NOTE: The HTTP username and password should be the same as the NTP Software QFS service account.

6. Click **OK** in the **NTP Software QFS Configuration** screen.

Setting the NTP Software QFS Application Properties

1. Right-click **Quota & File Sentinel** under the main Windows server.

2. Click **Properties** on the pop-up menu.

3. On the **Email Configuration** tab, clear the **Inherit Email Configuration** box, check the **Enable Email Notifications** box, enter the correct information in each of the four text boxes as appropriate for your network, and click **OK**.

4. Now, let's move on to configuring Simple Network Management Protocol (SNMP), which helps to manage complex networks. Click the SNMP Configuration tab. Clear the box Inherit SNMP Configuration, check the Enable SNMP Messages box, enter the SNMP console IP address that will be used to monitor the network, enter the community name, and click **OK**.

5. Click the **Event Options** tab and clear the **Inherit Options** box.

6. Next, we will configure the desired quota threshold and file management threshold events. Quota thresholds post events when falling below thresholds, when exceeding thresholds, or both. Check the desired settings in the Quota Threshold Events section of the dialog box. File management thresholds post events for file management time remaining thresholds, file deletion operations, or both. Check the desired settings in the **File Management Threshold Events** section of the dialog box.

7. Click the **Security** tab. Clear the **Inherit Security** box and check the **Enable Security** box. Click **Add** to choose the members or groups for which you want to apply security options.

   > **NOTE:** In the **Non-Owner Permissions** section of the dialog box, choose the desired settings for the types of policies and properties.

8. Click the **Hitachi Connector** tab to add/remove the Hitachi NAS(es) to be managed by the Hitachi Connector, quarantine/delete prohibited files, and enable/disable file-blocking recovery.

   - The share QFSQuarantine or QFSQuar must exist on each managed machine so Quarantine can work properly.

   - The Quarantine and Delete options work with DeepScan® and ZipScan™, so if a file is considered "denied" after it was deep-scanned or zip-scanned, it will be deleted or quarantined depending on the selected option.

   - Enabling the file-blocking recovery settings allows quarantining or deleting the prohibited files by NTP Software QFS file control policies that were copied while the NTP Software QFS Connector service wasn't running. This can happen if the QFS machine was rebooted or shutdown for any reason.

9. Click the **Misc. Options** tab to configure daily email reminders for users who are at or near quota, directory connector properties (for resolving email addresses), and tuning properties, which control how NTP Software QFS sizes objects at system startup.

   - The daily reminder feature works in conjunction with the **Send to Triggering User** setting on the **General** tab of the **Threshold Properties** dialog box. If you're not sending email notifications to users when an object reaches its quota, the daily reminder setting has no effect, whether you've enabled it or not.

   - If the AM/PM field is set to AM, and you enter 12-23 (military time) in the Hour field, the AM/PM field changes to PM, and the hour adjusts itself to regular time (12-11 PM).

   - The **Inherit Directory Connector Properties** option works in conjunction with the **Email Configuration** tab on the **NTP Software QFS Configuration** dialog box. If you disable email notifications on the **Email Configuration** tab, the following options are also disabled.

Sizing Options

NTP Software QFS allows administrators to decide whether to calculate space using the logical size of files or the physical size of files, where space calculation using logical size is determined by the size of the data found in files and space calculation using physical size is determined by the actual amount of disk allocation units the file consumes. So physical sizing simply refers to the size on disk. This can be performed as follows:

1. Right-click Quota & File Sentinel under the main NAS device or a non-Windows server container.

2. Click **Properties** on the pop-up menu.

3. On the **Size Options** dialog box, clear the **Inherit Size Options** box if you want to set the sizing option individually on a NAS device. In this case, you need to choose whether to calculate using each file's logical size for all files or calculate using each file's physical size for all files.

    - If the size option is changed, this will force a resize operation to occur on the NAS device. NTP Software QFS will continue to enforce quotas based on the previous size selection until the resize operation is complete.

    - The default size option is a logical sizing option.

    - The sizing option is not available on Windows hosts machines. Logical sizing is used for all Windows hosts.

NOTE: While QFS for NAS can size by logical or physical file sizes, QFS for Windows cannot.

Policy Creation

This section outlines standard NTP Software QFS procedures for creating policies.

Please note:

- NTP Software QFS manages two main types of paths: directory paths and share paths. For share paths, all you need to do is add a share name. For directory paths, the format depends on the NTP Software QFS edition being used.
  - For NAS NetApp edition, the directory path format is \vol\<volume name>\<some directory>[…\optional subdirectory\another optional subdirectory]
  - For NAS EMC, the directory path format is \<file system mount path>\<some directory>[…\optional subdirectory\another optional subdirectory]
  - For Hitachi edition, the directory path format is \fs\<volume name>\<some directory>[…\optional subdirectory\another optional subdirectory]
  - For Windows edition, the directory path format is Drive:\<some directory>[…\optional subdirectory\another optional subdirectory]

    Examples: d:\private\marketing or d:\users\*

- Directory paths can have different behavior by putting a star '*' instead of one of the directory names. This type of path forms a star policy, which can be used to manage all directories in the level of the '*'.

  Important: As QFS for NAS allows the use of * in the middle of a managed path, QFS for Windows does not.

  When testing policies you have created, perform the tests from an independent machine that is not running NTP Software QFS.

Copyright © 2000-2015 NTP Software

Creating Disk Quota Policies

This section walks you through creating a typical disk quota policy. We will create a quota policy for all your user home directories in a typical server configuration. This quota policy will be applied to all users in your Users directory. Each user will get a quota limit of 50MB.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server/Filer/CIFS Server/EVS you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to Quota & File Sentinel to expand the policy types.

2. Right-click Disk Quota Policies and select New > Folder Policy Using Directories.

3. In the New Policy dialog box, click the General tab. Enter a name and a description for your new policy.

4. Click the **Quota** tab, select **Absolute Quota Limit**, enter 50 MB as the limit, click **Deny Writes at 100% of quota**, and leave **Overdraft** unchecked for this example.

> **NOTE:** In a production environment, it is a best practice to implement a 10% overdraft.

5. Click the **Thresholds** tab to view the thresholds for this quota policy. Notice that one threshold is already set up: At Quota 100%. Adding more thresholds is as simple as clicking **Add** and filling in the percentage information for that threshold.

As space is consumed, these thresholds serve as triggers for various actions. Each threshold can send email or pop-up messages to the triggering user, the NTFS owner of the file, and/or to any other group or individual (network administrators, the Help Desk, and so on). A threshold can also run a third-party process– for example, running a virus scan on the file in question, or starting an archive to tape.

NTP Software QFS lets you create up to 200 threshold levels for each policy. Common choices for additional levels are 75%, 85%, and 95%. As users hit each of these levels, you can customize your messages to suggest that users delete some files or contact the Help Desk and request a quota increase before their ability to save new documents runs out. It is also possible to integrate NTP Software QFS with your intranet or automated workflow and process the limit increase automatically.

6. Double-click the At Quota 100% threshold. The Threshold Properties dialog box for that threshold level appears. If you configured NTP Software QFS for email earlier, select the checkbox for email to the triggering user.

The **Messages** tabs let you customize the text of the messages that will be sent.

The **Threshold Commands** tab allows you to specify a program, script, or batch (.BAT) file that will run when the threshold is reached.

7. After you have chosen the appropriate settings for email and messages, click OK to return to the **New Policy** dialog box.

8. Click the **Directories** tab. Click the **Add** button, type the appropriate directory path for your Users directory followed by a backslash and asterisk (*), or type the directory path with an asterisk (*) in the middle of the path to manage a subpath under each user directory. For asterisks in the directory path, only one asterisk is allowed.

   Important: As QFS for NAS allows the use of * in the middle of a managed path, QFS for Windows does not.

   > **NOTE:** By default, this quota applies to all users. You can verify this fact by clicking the **Managed Users and Groups** tab.

Administrators, Backup Operators, Replicator, and the System account are exempt from quotas. You can verify this fact by clicking the **Exempt Users and Groups** tab. To change this setting, select the appropriate entry and click **Remove**.

9. Click the **Exempted Directories** tab. Click the **Add** button, type the subdirectory you want to exempt from the managed directories list.

   > **NOTES:**
   >
   > - Asterisks * are not supported to be part of the exempted path.
   > - While QFS for NAS can exclude directories from quota policies, QFS for Windows cannot.

10. Click **OK** to close the **New Policy** dialog box. NTP Software QFS will create the new quota directory policy, which will be inherited by all systems from this point down in your hierarchy.

Creating File Control Policies

This section shows you how to create a file control policy. Perhaps your company has a corporate policy that forbids downloading music files from the Internet. To help the staff comply with this policy, let's create a file control policy that prohibits creating music files on the server.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server/Filer/CIFS Server/EVS you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to Quota & File Sentinel to expand the policy types.
2. Right-click **File Control Policies** and select **New** > **Folder Policy Using Directories**.
3. The **New File Control Policy** dialog box opens. Give your policy a name and description.
4. Click the **Criteria** tab. Then click **Add** and enter the file patterns you want to block (for example, *.AVI, *.MP3, *.MPG, *.MP2, and *.VBS).

NOTE: Be sure to include the asterisk and period (*.) when you specify a file type.

NTP Software QFS follows the normal Windows rules for wildcard file specifications. For example, enter *.MP? to include .MP3, .MP2, .MPG, etc. — all music files.

Important: As QFS for NAS allows the use of * in the middle of a managed path, QFS for Windows does not.

This tab also includes two options, **Block Zip files** containing prohibited content and **Enable NTP Software DeepScan Technology**, which enable the administrator to decide how thoroughly files are scanned for the policy. See the following sections of this document for more detailed information on these features.

5. Click **OK** to return to the **New File Control Policy** dialog box.
6. Click the **Directories** tab. Click the **Add** button, and either type the directory path or type the appropriate directory name followed by a backslash and asterisk (*).
7. Click the **Control Options** tab. Because our policy is to prevent the creation of these files, select the radio button labeled **Always Deny** under the options **Open for Read**, **Open for Write**, and **Create New**.
8. By default, user accounts with Administrator privileges are exempt from any policy you create. If you want to change this setting, click the **Exempt Users and Groups** tab, select the **Administrators** entry, and click **Remove**.
9. Click **OK** to save this policy.

Creating File Management Policies

This section walks you through creating a file management policy. Your company may have a corporate policy that allows your employees to store files in a central or shared location. As an administrator, you are responsible for maintaining the data stored in this location, which includes deleting old or obsolete data. Let's create a file management policy that automatically manages aged files.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server/Filer/CIFS Server you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign next to Quota & File Sentinel to expand the policy types.

2. Right-click **File Management Policy** and select **New** > **Folder Policy Using Directories**.

3. The **New File Management Policy** dialog box opens. Give your policy a name and description.

4. Click the **Criteria** tab. Set the aspects of the policy: file patterns to remove, age of the files, size, and archive status. You can also select a specific action to take for the files– for example, allowing audit, quarantine, or removal when the policy is triggered. Specify when to enforce the policy and whether it will be applied retroactively to files created before the policy.

   NOTE: When the file management policy is configured to "remove" old or obsolete date, it will remove empty directories after processing them. If a managed directory was not empty and the file removal policy controlling it has deleted all files in the managed directory, the policy will remove this directory if the **Remove Empty Directories** option is checked.

5. Click the **Alerts** tab. As desired, turn on alerts for the quarantine and deletion of files. Once the alert is enabled, you have the option of enabling email (if the email server has been configured).

6. Click **OK** to save the policy.

Viewing Directories

This section shows how you can view all the directories that are located on a certain server, Filer, CIFS Server, Titan, or Hitachi NAS.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server, Filer, or CIFS Server containing directories you want to view. If necessary, click the plus sign (+) adjacent to this entry to expand the tree.

2. Click the plus sign next to Quota & File Sentinel.

    a. For the Windows server, click the plus sign (**+**) next to **Server Directories** to view the folders located on that server.

    b. For the Filer, click the plus sign (+) next to Filer Directories to view the volumes located on that Filer.

    > **NOTE:** You can view that feature if you have a NetApp Filer attached to the NTP Software QFS application.

    c. For the CIFS Server, click the plus sign (+) next to CIFS Server Directories to view the file systems located on that CIFS Server.

    > **NOTE:** You can view that feature if you have an EMC CIFS Server attached to the NTP Software QFS application.

Viewing Shares

This section shows how you can view all the shared directories located on a certain server, Filer, or CIFS Server.

1. In the NTP Software Smart Policy Manager hierarchy view, locate the server, Filer, or CIFS Server with shared directories you want to view. If necessary, click the plus sign (+) adjacent to this entry to expand the tree.

2. Click the plus sign (+) next to Quota & File Sentinel.

    d. For the Windows server, click the plus sign (+) next to Server Shares to view the shared folders located on that server.

    e. For the Filer, click the plus sign (+) next to Filer Directories to view the volumes located on that Filer.

    > **NOTE:** You can view that feature if you have a NetApp Filer attached to the NTP Software QFS application.

    f. For the CIFS Server, click the plus sign (+) next to CIFS Server Shares to view the shared folders located on that CIFS Server.

    > **NOTE:** You can view that feature if you have an EMC CIFS Server attached to the NTP Software QFS application.

NTP Software DeepScan®

A powerful feature of NTP Software QFS is NTP Software DeepScan®. This technology allows the administrator to specify whether to use the default scan for file extensions, or scan deeper for header information to determine the true nature of a file.

Before selecting **Enable Deep Scan Technology** on the **Criteria** tab in the **New File Policy** dialog box, it is important that you understand how this function will affect your data and user community.

NTP Software DeepScan uses file header information to determine the type of file. Even if the file *Sunshine on My Shoulder.mp3* is renamed *Sunshine on My Shoulder.txt*, it will be seen and controlled as an audio (.MP3) file. Likewise, *Lion.jpg* may be renamed to *Lion.txt*, but it still will be seen and controlled as a .JPG file. NTP Software DeepScan does this by looking at the file's type. A .JPG file is in JPEG image format, so it will not matter whether the file has the extension .JPG, .JPEG, or .TXT.

NTP Software DeepScan supports the following file types:

- Audio Files. NTP Software DeepScan supports audio files with extensions .AIF, .AIFF, .IFF, .AU, .SND, .CDA, .WMA, .ASF,.MIDI, .FLAC, .OGG, .RMI, .RA, .RAM, .RM, and .AA

- Video files. NTP Software DeepScan supports video files with extensions .MOV, .QT, .MPEG, .MPG, .WMV, .ASF, .M4V, .RM.

- Other files. NTP Software DeepScan supports files with extensions .M3U, .MID, .M4V, .MPEG4, .MPEG2, .RAR, .MP33, .MP3A, .MP3B.

Some notable items regarding NTP Software DeepScan operations are the following:

- Microsoft Office files. Microsoft Office applications store documents as OLE structured storage files (known as compound files). Microsoft Office recognizes Office files regardless of extension (.PST, .DOC, .XLS, etc.), and they are all treated as the same file type. This characteristic prevents NTP Software QFS from being able to block .PST files while allowing .DOC files, for example, when NTP Software DeepScan is enabled. The .DOC file is seen as the same file type as the blocked .PST and is also blocked. If the administrator adds .DOC to managed files, NTP Software QFS will also manage other Office files in the same manner.

- Microsoft Office 2007 files. Those files are real .ZIP files. So, if .ZIP files are to be controlled by the NTP Software DeepScan, the MS Office 2007 files will be controlled under the category of .ZIP files, too.

- Text files. When forming your file control strategy, bear in mind that a .VBS or .BAT file is a text format file. With NTP Software DeepScan enabled, NTP Software QFS will manage them (and similar text file extensions) in the same manner as .TXT files.

- Google Earth Keyhole markup files. The same limitation that applies on MS Office 2007 files applies on Google Earth Keyhole markup files.

- Windows installer files. MSI files will be recognized as MS Office files because of the format MS implemented them in.

To enable NTP Software DeepScan, perform the following steps:

1. In the NTP Software Smart Policy Manager hierarchy view, locate the Filer or CIFS Server you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign (+) next to Quota & File Sentinel to expand the policy types.

2. Expand the File Control Policies. Then right-click the desired file control policy and select Properties.

3. Click the **Criteria** tab. Check the **Enable NTP Deep Scan Technology** option to control how thoroughly files are scanned for the policy.

NTP Software ZipScan™

Another powerful feature of NTP Software QFS is NTP Software ZipScan™. If this option is selected, NTP Software QFS looks for managed file types inside compressed files with the .ZIP extension. For example, entering the .MP3 file type and selecting **Block Zip files containing prohibited content** on the **Criteria** tab in the **New File Policy** dialog box will block files named .MP3 within a .ZIP file.

Blocking .ZIP files is performed by examining the list of contents for the .ZIP file. With current technology, adding a third level of scanning could negatively impact file operations. When polling the industry, we found that most customers were not particularly concerned with renamed files within .ZIP files because users would find using those renamed files to be cumbersome enough to outweigh any benefits they would gain.

To enable NTP Software ZipScan, perform the following steps:

1. In the NTP Software Smart Policy Manager hierarchy view, locate the Filer or CIFS Server you added earlier. If necessary, click the plus sign (+) adjacent to this entry to expand the tree. Then click the plus sign (+) next to Quota & File Sentinel to expand the policy types.

2. Expand the File Control Policies. Right-click the desired file control policy and select Properties.

3. Click the **Criteria** tab. Check the **Block Zip files containing prohibited content** option to specify how thoroughly files are scanned for the policy.

NTP Software End User Support Infrastructure™ (NTP Software EUSI™)

NTP Software End User Support Infrastructure™ (NTP Software EUSI™) is an integrated component of NTP Software's QFS application. EUSI contains several utilities to aid network administrators in informing users about what constitutes a quota violation and to assist users in fixing the problem.

To install NTP Software EUSI, insert the DVD and select the installation option from the install interface. Follow the prompts to install the various components:

- NTP Software QFS Email Templates. Install these components on the same server as NTP Software QFS.

- NTP Software Storage HelpSite. This collection of web pages describes what each quota policy violation means. Its purpose is to help users understand why they were notified about a quota violation, to reduce the amount of time administrators spend answering these simple questions.

- NTP Software EUSI website. This site allows users to see what policy they violated, request policy changes, and clean up their drives.

The NTP Software Storage HelpSite, EUSI website, and NTP Software Storage Investigator™ components should be installed on an intranet web server. The NTP Software QFS Email Templates component should be installed on the server in which NTP Software QFS is installed.

Three dialog boxes are of particular importance in the installation process:

- Virtual Directory. When the NTP Software Storage HelpSite and NTP Software EUSI website are installed on a web server, the installation creates virtual directories. By default, the directories are named HelpSite and EndUserSupportWebSite. You can change these default names in the Virtual Directory dialog box.

- Hosting URL. Use this dialog box to specify the URL of the web server that hosts the NTP Software Storage HelpSite and NTP Software EUSI website. For example, use the following addresses:

  http://10.10.2.40

  http://intranetserver

This address is used by the NTP Software QFS Email Templates component to access the websites.

- E-mail Options. In this dialog box, the Recipient is the mailbox to which quota change requests should be sent. One feature of the NTP Software EUSI website is the capability for users to email requests for quota policy changes. The SMTP server is the address of the email server to use.

NTP Software QFS Email Templates

NTP Software QFS Email Templates are preformatted HTML email messages that can be imported easily into NTP Software QFS. The following email templates are provided:

- BelowThreshold. Indicates that the user has gone below quota and is now allowed to save things to the share name again.

- FileBlocked. Indicates that a particular file was blocked from being stored on a network share. This message might indicate a prohibited extension (such as .MP3) or some other blocking reason specified in the NTP Software QFS policy.

- OverQuota. Indicates that a user's action has caused his or her storage to exceed quota. This particular message contains links to both the NTP Software Storage HelpSite and the NTP Software EUSI website. The OverQuota email message automatically passes the server and share name of the drive on which the quota was violated. To change this setting, see the NTP Software QFS documentation for valid keys.

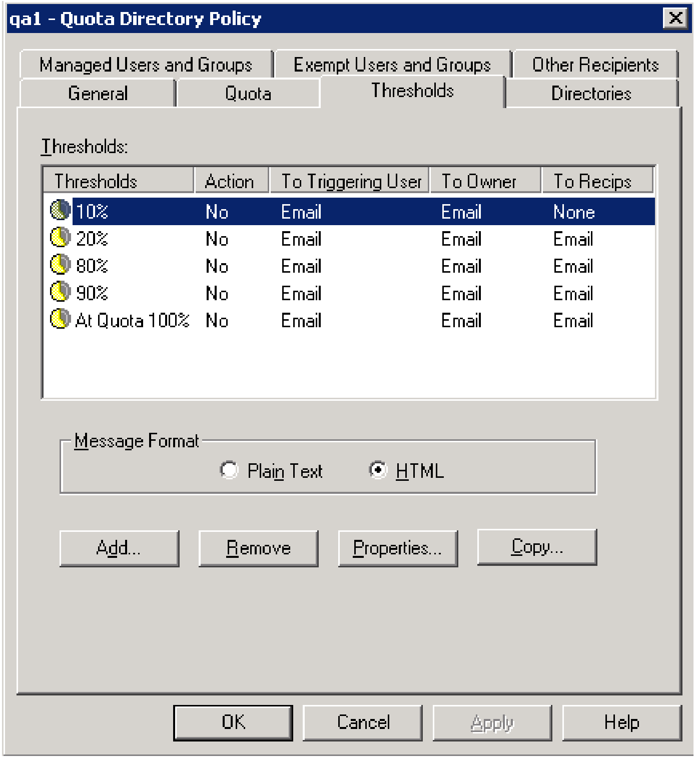
- FileRemoval. Indicates that a particular file of a user has been removed by a file removal policy.

NOTE: When installing the NTP Software QFS Email Templates, it is very important that you specify URLs for the NTP Software Storage HelpSite and the NTP Software EUSI website. The default web pages have placeholders for these URLs. If you do not specify the addresses, the email templates will not function as designed.

Adding an Email Template to NTP Software QFS

1. Open the NTP Software QFS Admin tool. Select the policy to which you want to add email; then choose File > Properties.

2. Click the **Thresholds** tab.



Thresholds:

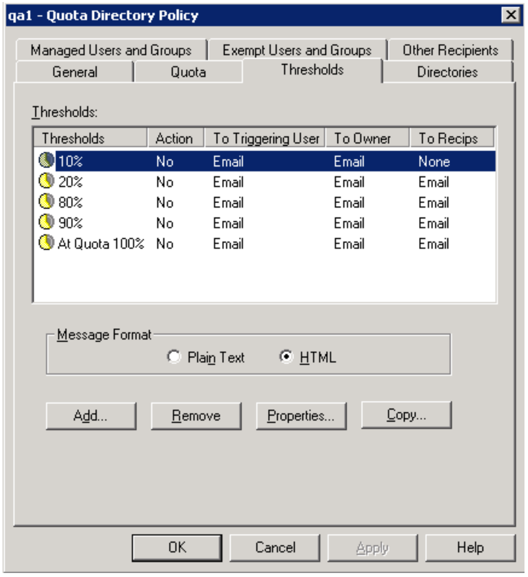
Thresholds	Action	To Triggering User	To Owner	To Recips
10%	No	Email	Email	None
20%	No	Email	Email	Email
80%	No	Email	Email	Email
90%	No	Email	Email	Email
At Quota 100%	No	Email	Email	Email

Message Format: ○ Plain Text ● HTML

3. Select **HTML** as the message format and then click the **Properties** button.

4. In the **Threshold Properties** dialog box, you can customize messages for each type of recipient. For this example, we want to send email only to the user who triggered the quota. In the **Send to Triggering User** section of the dialog box, select **Email** as the notification method.

5. Click the **Triggering User Messages** tab.

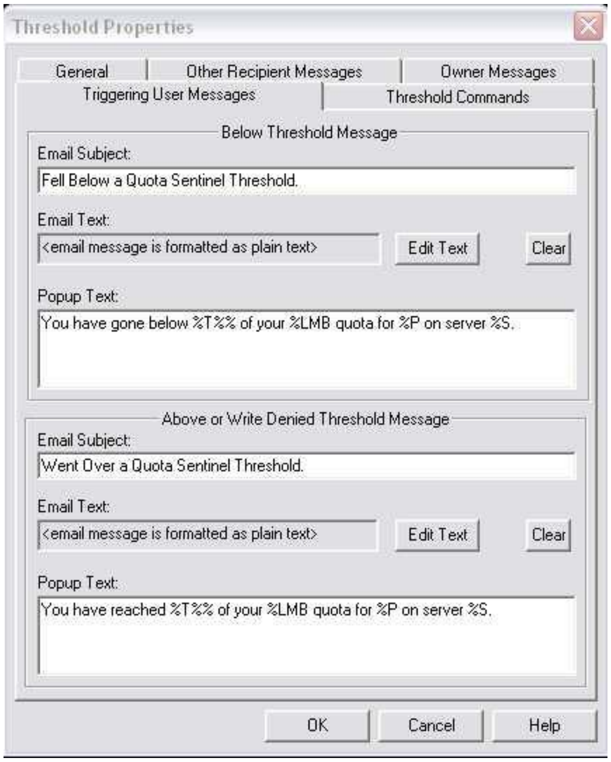


Thresholds:

Thresholds	Action	To Triggering User	To Owner	To Recips
10%	No	Email	Email	None
20%	No	Email	Email	Email
80%	No	Email	Email	Email
90%	No	Email	Email	Email
At Quota 100%	No	Email	Email	Email

Message Format: ○ Plain Text ● HTML

6. In the section **Above or Write Denied Threshold Message**, click the **Edit Text** button to open a text editor. In the text editor, choose **File** > **New** to remove all existing text.



Below Threshold Message

Email Subject: Fell Below a Quota Sentinel Threshold.

Email Text: <email message is formatted as plain text>

Popup Text: You have gone below %T%% of your %LMB quota for %P on server %S.

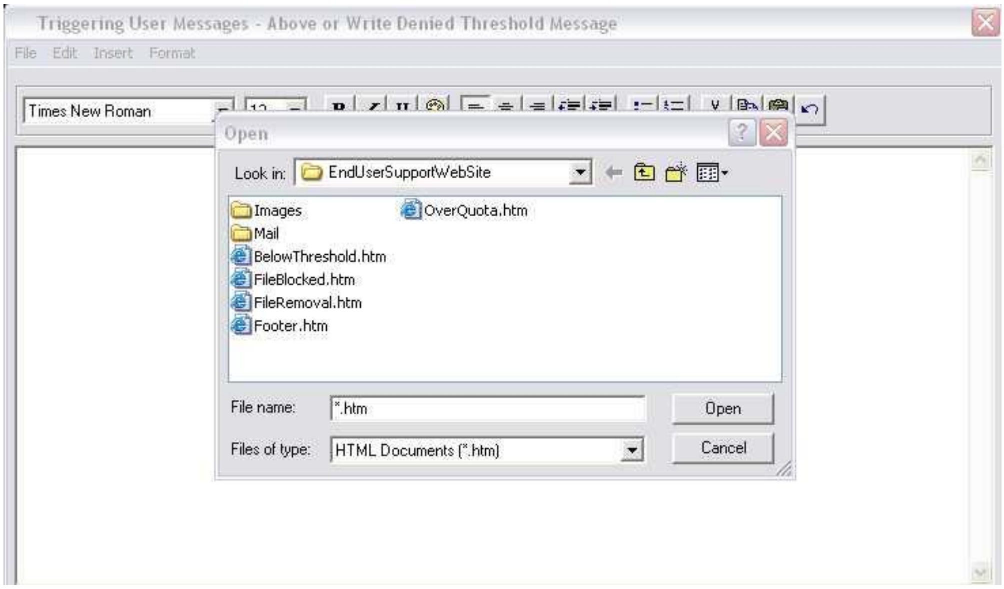
Above or Write Denied Threshold Message

Email Subject: Went Over a Quota Sentinel Threshold.

Email Text: <email message is formatted as plain text>

Popup Text: You have reached %T%% of your %LMB quota for %P on server %S.

7. Choose **Insert** > **File**. Browse to the directory where NTP Software EUSI website was installed and open the file OverQuota.htm.


Triggering User Messages - Above or Write Denied Threshold Message
File
Edit
Insert
Format
Times New Roman
Open
Open
Cancel

Look in: EndUserSupportWebSite

Images
Mail
BelowThreshold.htm
FileBlocked.htm
FileRemoval.htm
Footer.htm
OverQuota.htm

File name: *.htm

Files of type: HTML Documents (*.htm)

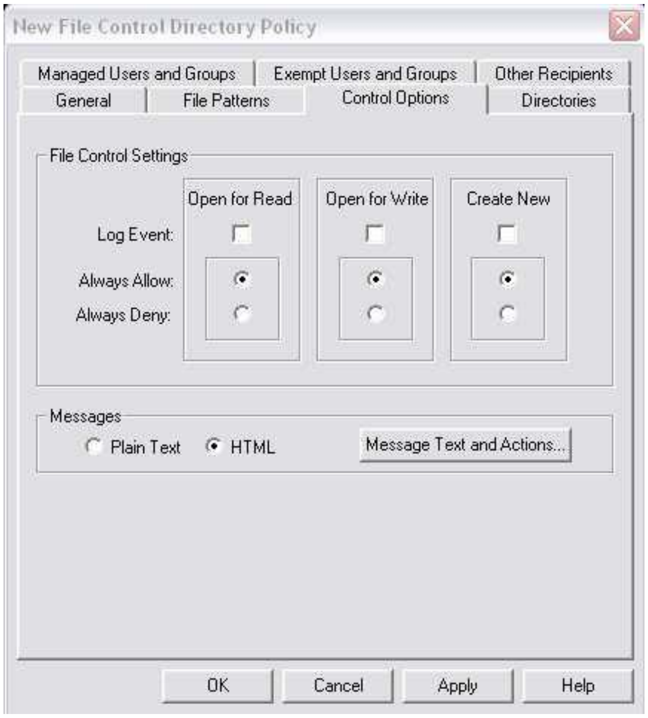
8. Click **File, Save, & Close**.

9. Click **OK** as needed to exit the dialog boxes. Now, when a user goes over quota, he or she will receive an email message explaining that the quota limit has been reached on that server.

Specifying a File Control Message

1. After creating a file control directory policy, click the **Control Options** tab in the **New File Control Directory Policy** dialog box.

2. In the **Messages** section of the dialog box, select **HTML**. Then click the **Message Text and Actions** button.



File Control Settings

	Open for Read	Open for Write	Create New
Log Event:	□	□	□
Always Allow:	●	●	●
Always Deny:	○	○	○

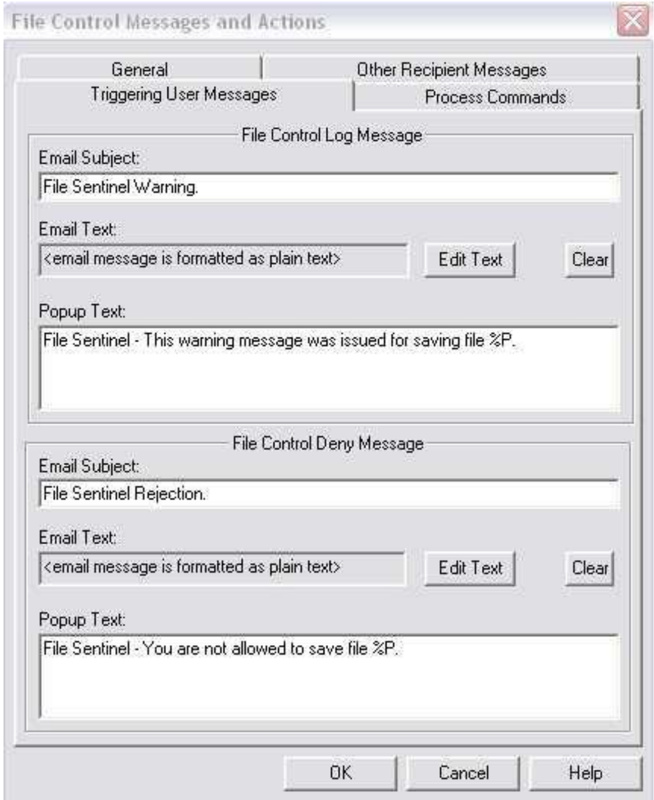
Messages

○ Plain Text ● HTML [Message Text and Actions...]

3. In the **File Control Messages and Actions** dialog box, click the **General** tab and select **Email** as the notification method in the **Send to Triggering User** section of the dialog box.

Copyright © 2000-2015 NTP Software

4. Click the **Triggering User Messages** tab. In the **File Control Deny Message** section of the dialog box, click the **Edit Text** button to open a text editor. In the text editor, choose File > New to remove all existing text.



File Control Log Message

Email Subject: File Sentinel Warning.

Email Text: <email message is formatted as plain text>

Popup Text: File Sentinel - This warning message was issued for saving file %P.

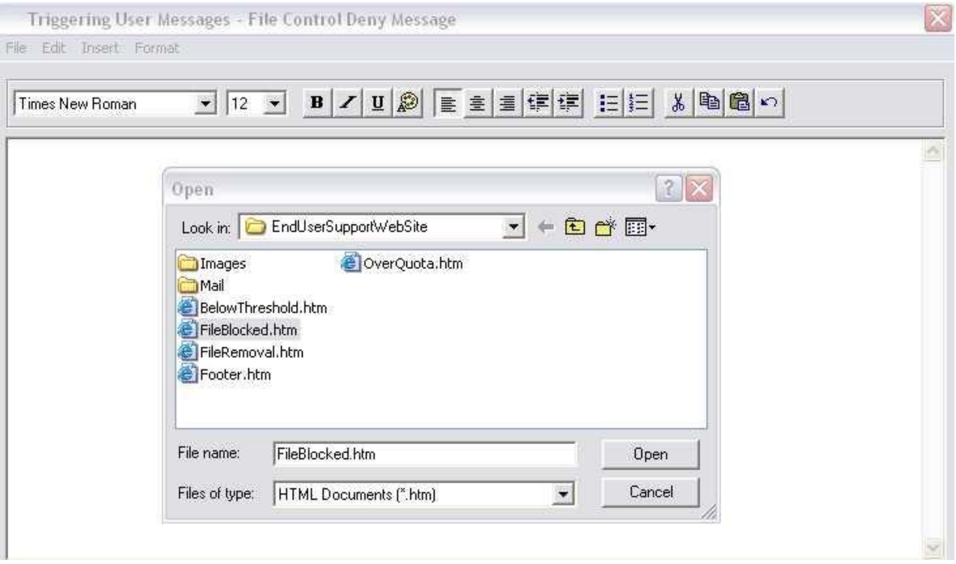
File Control Deny Message

Email Subject: File Sentinel Rejection.

Email Text: <email message is formatted as plain text>

Popup Text: File Sentinel - You are not allowed to save file %P.

5. Choose **Insert** > **File**. Browse to the directory where NTP Software EUSI website was installed and open the file FileBlocked.htm.



File name: FileBlocked.htm

Files of type: HTML Documents (*.htm)

6. Click **File, Save, & Close**.

7. Click **OK** as needed to exit the dialog boxes. Now, when a user tries to copy a blocked file, he or she will receive an email message.

NTP Software Storage HelpSite

The NTP Software Storage HelpSite provides web pages that answer the most basic questions about NTP Software QFS policies and violations. The idea is to take this burden away from the network administrator and put the information in one central place. The NTP Software QFS Email Templates contain links to the NTP Software Storage HelpSite so that when a user triggers an NTP Software QFS policy, he or she can quickly obtain information about the policy and how to fix the problem.

The NTP Software Storage HelpSite should be installed on a local web server. The installation process takes care of creating the virtual directory within IIS.

NTP Software End User Support Infrastructure Website

This website contains pages that allow the user to perform the following:

- Download NTP Software Storage Investigator for cleaning up the user's directories.
- Email the network administrator, requesting a change to the user's policy.

The website is accessible from the NTP Software QFS Email Templates files. During the installation of NTP Software EUSI, you will be prompted for the name of the virtual directory that should be created. This component should be installed on a web server.

NTP Software Storage Investigator™

NTP Software Storage Investigator™ is a tool to help users clean up their shares and directories in order to avoid violating storage policies. NTP Software Storage Investigator shows all files sorted by various criteria, such as the following:

- Largest files
- Oldest files
- Duplicate files
- Aged files
- Extensions

NTP Software Storage Investigator is an ActiveX control that is set up to download from CleanupFiles.asp on the NTP Software EUSI website. Due to the nature of ActiveX controls, the user must be an administrator on the local machine to download and register the ActiveX control. For environments in which users are not administrators on their local machines, an .MSI file is provided. This file can be used with Active Directory or other tools to “push” an installation of NTP Software Storage Investigator to each machine. Once the NTP Software Storage Investigator ActiveX control is installed and registered, users can run the control.

For more information on configuring NTP Software Storage Investigator, see *NTP Software Storage Investigator Parameters Reference*. For more information on using NTP Software Storage Investigator, see *NTP Software Storage Investigator User Manual*.

Administering NTP Software QFS Service through a NTP Software QFS Admin Client Running on a Different Machine

This section provides step-by-step instructions on installing the NTP Software QFS Admin Client, enabling you to administrate a QFS service running on a different machine. This kind of NTP Software QFS Admin Client installation enables NTP Software QFS administrators easily to administer NTP Software QFS that is installed on all the servers over the entire network. This can be done through a local user interface that is easily installed on the administrator's local machine.

For an NTP Software QFS administrator to be able to use the NTP Software QFS Admin Client, NTP Software Smart Policy Manager Admin and NTP Software QFS Admin components should be installed on the administrator's local machine as per the following instructions.

NOTES:

- There is a slight difference in the installation of NTP Software Smart Policy Manager and NTP Software QFS on an NTP Software QFS Server versus the installation on an administrator's local machine.

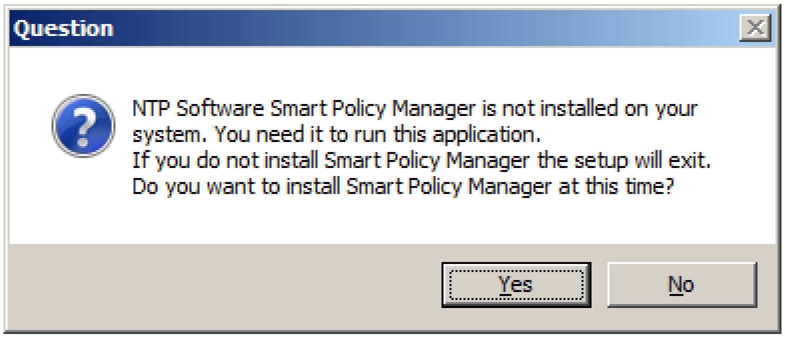
- NTP Software QFS Admin Client User Interface is using Remote RPC to communicate to the NTP Software Smart Policy Manager service. Therefore, NTP Software QFS Administrator needs to have permissions to run and execute Remote RPC on the managed machine. A standard user does not have RPC Permission by default. Therefore, if the user performing the administration is not an administrator in the domain, the user needs to be added to the Distributed COM Users group on the machine to be managed.

Installing NTP Software Smart Policy Manager Admin Component

1. Log on to your local computer, using an account with administrator privileges.

2. On the NTP Software Product Installation page, click your product installation link under the Product Components section.

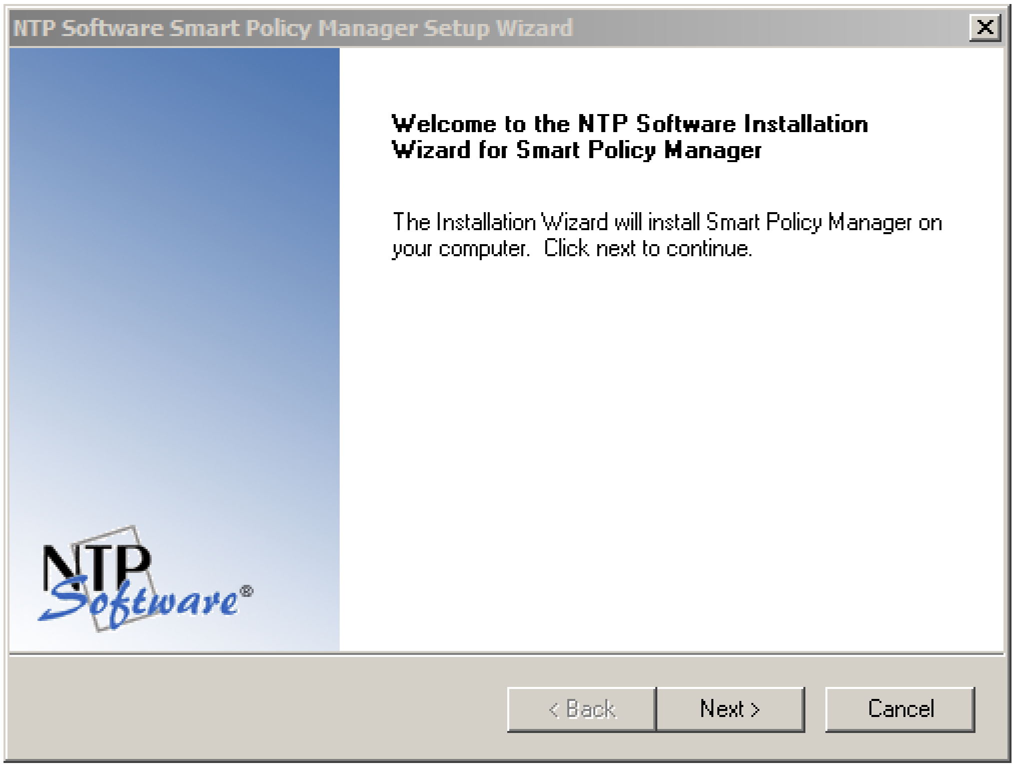
3. When prompted to install NTP Software Smart Policy Manager, click **Yes** to launch the Installation Wizard.



Question

NTP Software Smart Policy Manager is not installed on your system. You need it to run this application.
If you do not install Smart Policy Manager the setup will exit.
Do you want to install Smart Policy Manager at this time?

4. On the NTP Software Smart Policy Manager installation welcome dialog box, click **Next**.

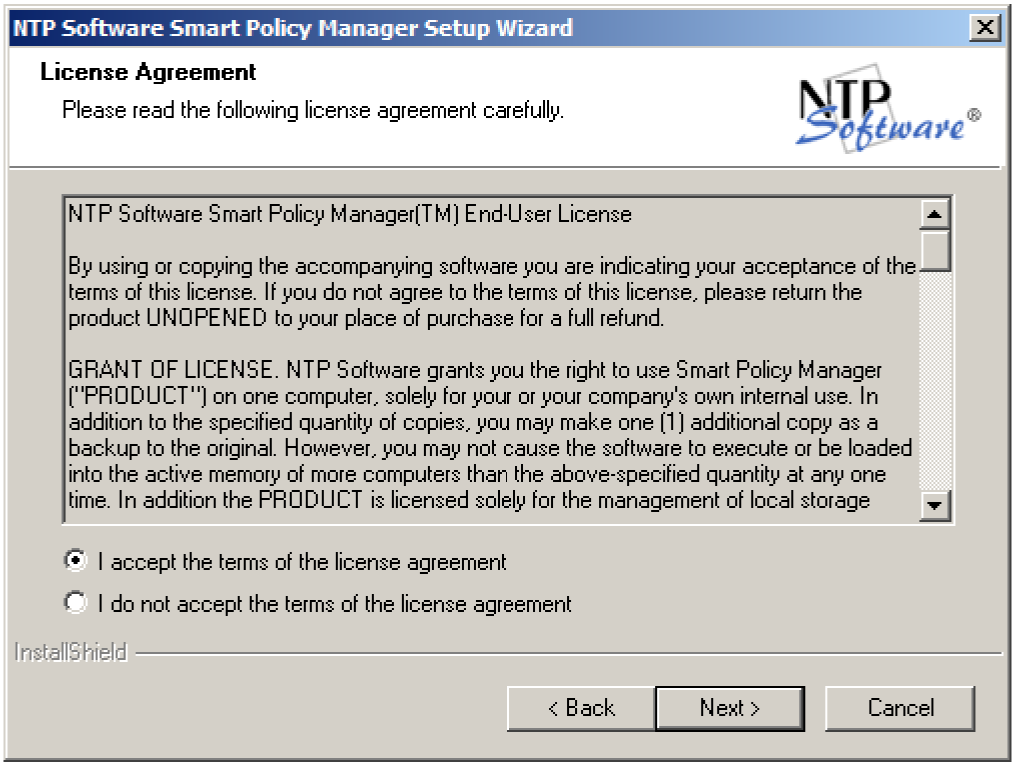


NTP Software Smart Policy Manager Setup Wizard

Welcome to the NTP Software Installation Wizard for Smart Policy Manager

The Installation Wizard will install Smart Policy Manager on your computer. Click next to continue.

5. Select **I accept the terms of the license agreement** in the License Agreement dialog box; then click **Next**.



License Agreement

Please read the following license agreement carefully.

NTP Software Smart Policy Manager(TM) End-User License

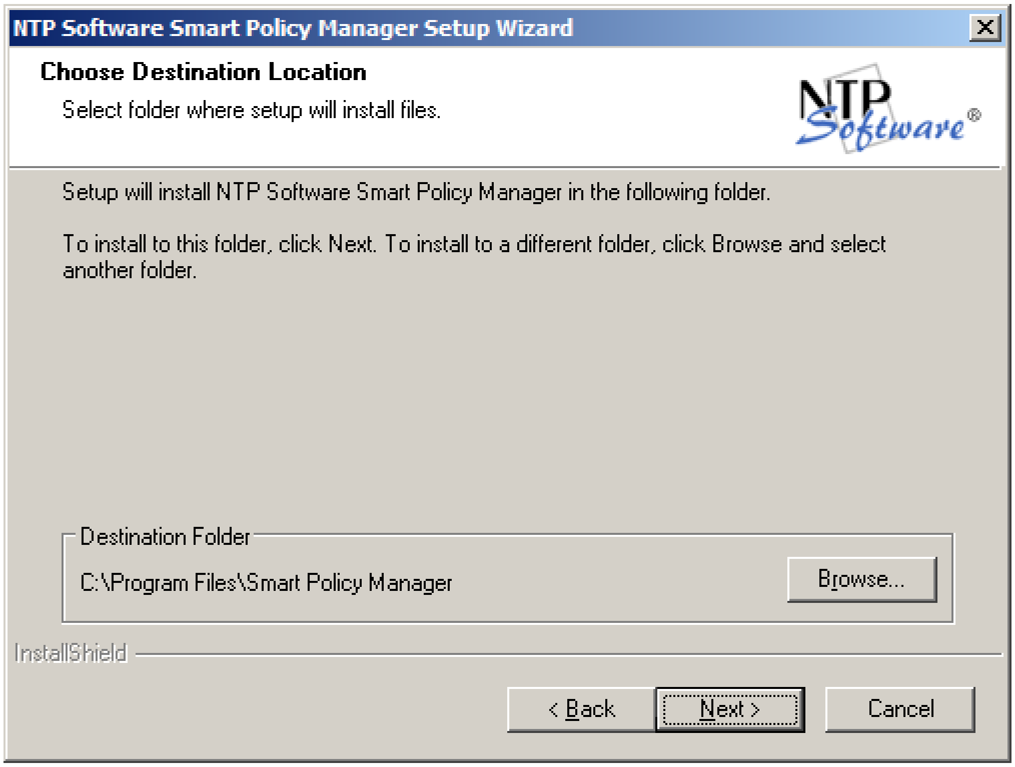
By using or copying the accompanying software you are indicating your acceptance of the terms of this license. If you do not agree to the terms of this license, please return the product UNOPENED to your place of purchase for a full refund.

GRANT OF LICENSE. NTP Software grants you the right to use Smart Policy Manager ("PRODUCT") on one computer, solely for your or your company's own internal use. In addition to the specified quantity of copies, you may make one (1) additional copy as a backup to the original. However, you may not cause the software to execute or be loaded into the active memory of more computers than the above-specified quantity at any one time. In addition the PRODUCT is licensed solely for the management of local storage

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

6. In the **Choose Destination Location** dialog box, browse to the needed location, then click **Next**.



Choose Destination Location

Select folder where setup will install files.

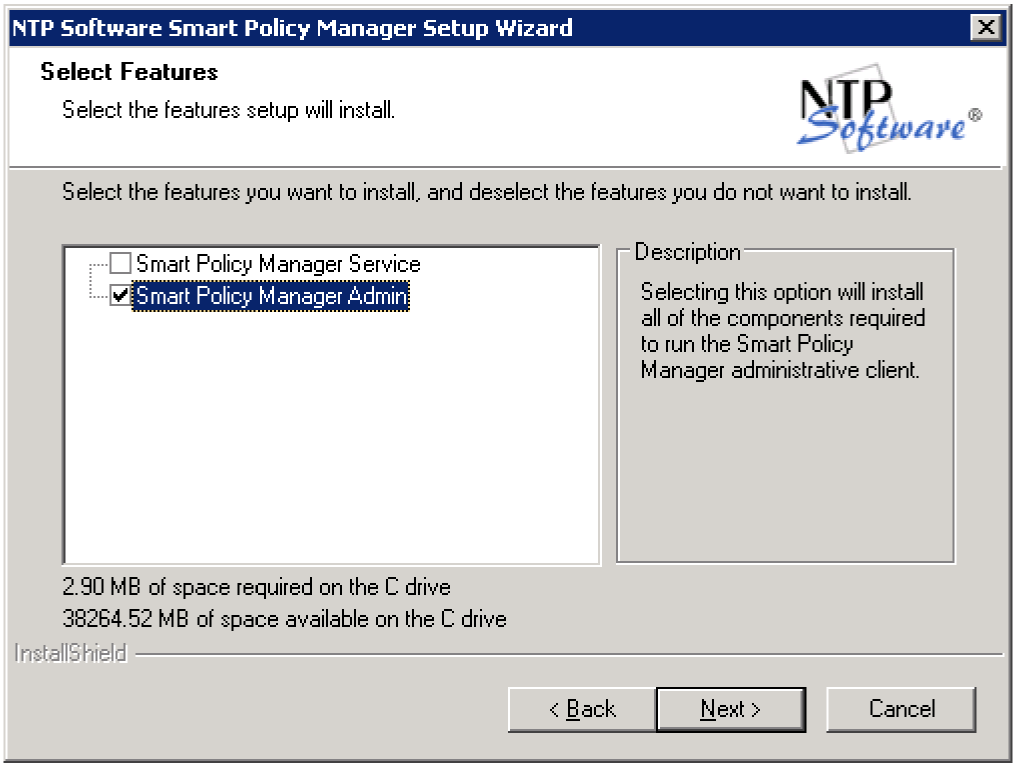
Setup will install NTP Software Smart Policy Manager in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\Smart Policy Manager

7. Select only the **Smart Policy Manager Admin** component in the **Select Features** dialog box. Click **Next**.



NTP Software Smart Policy Manager Setup Wizard

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☐ Smart Policy Manager Service
☑ Smart Policy Manager Admin

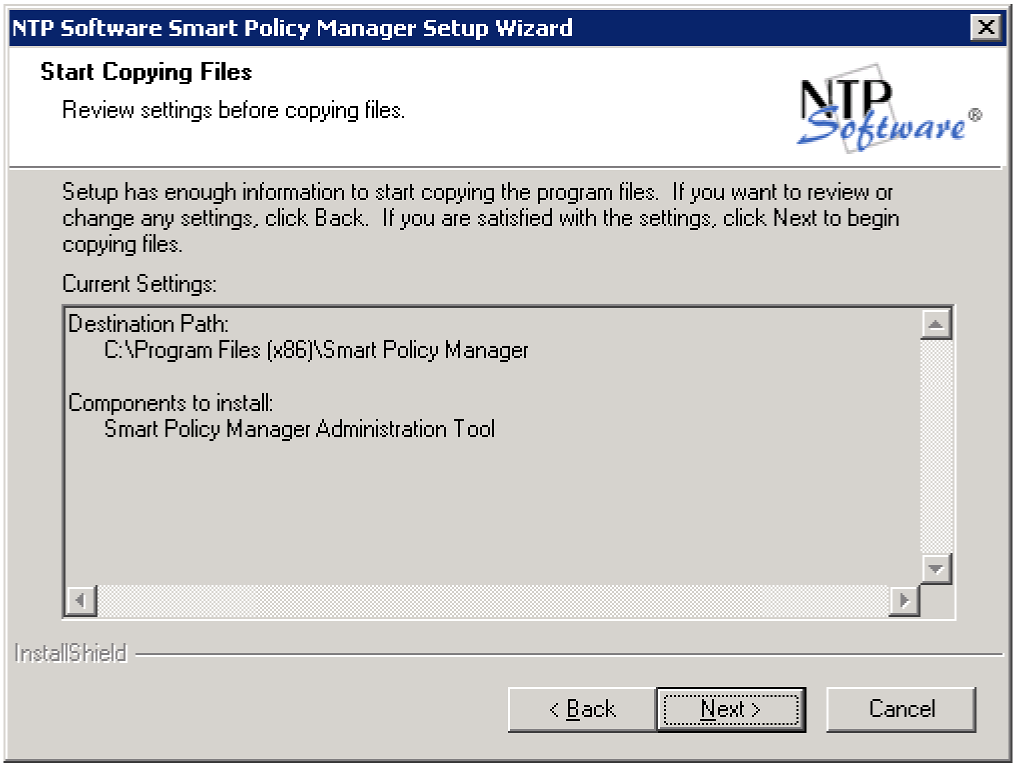
Description

Selecting this option will install all of the components required to run the Smart Policy Manager administrative client.

2.90 MB of space required on the C drive
38264.52 MB of space available on the C drive

Copyright © 2000-2015 NTP Software

8. The **Start Copying Files** dialog box prompts you to begin copying files.



Start Copying Files

Review settings before copying files.

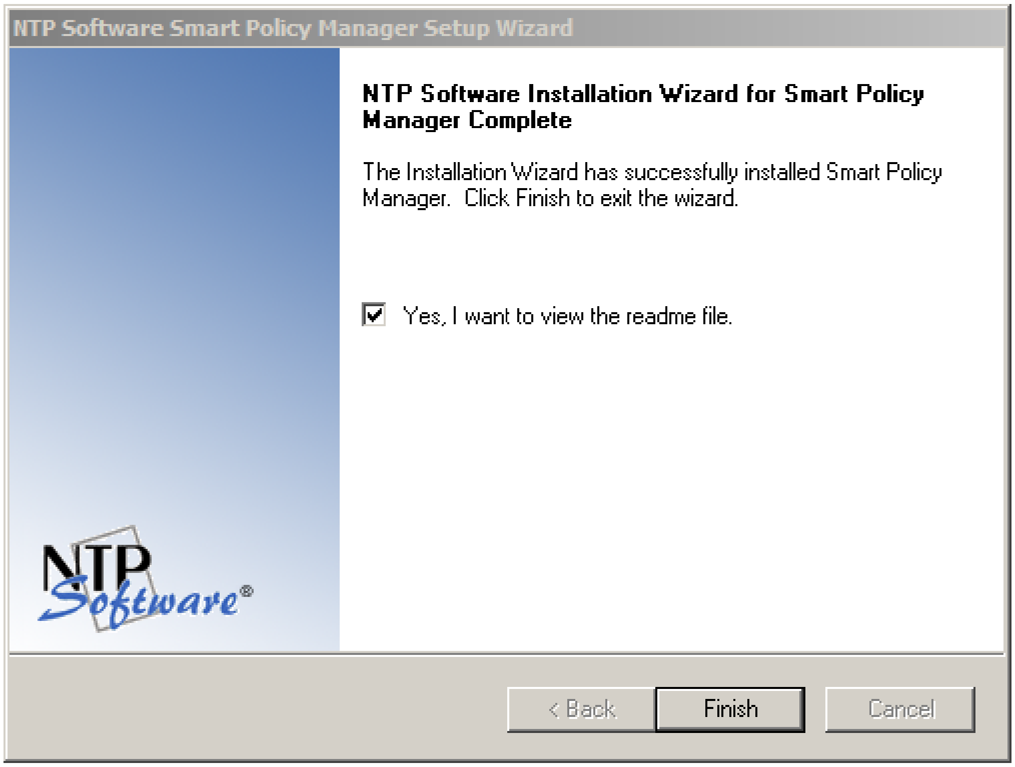
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

Current Settings:

```
Destination Path:
    C:\Program Files (x86)\Smart Policy Manager

Components to install:
    Smart Policy Manager Administration Tool
```

9. When the file installation is complete, a dialog box offers you the opportunity to view the readme file, which may contain documentation updates and other items. If you do not want to view the readme file at this time, clear the option **Yes, I want to view the readme file**. Click **Finish**.



NTP Software Smart Policy Manager Setup Wizard

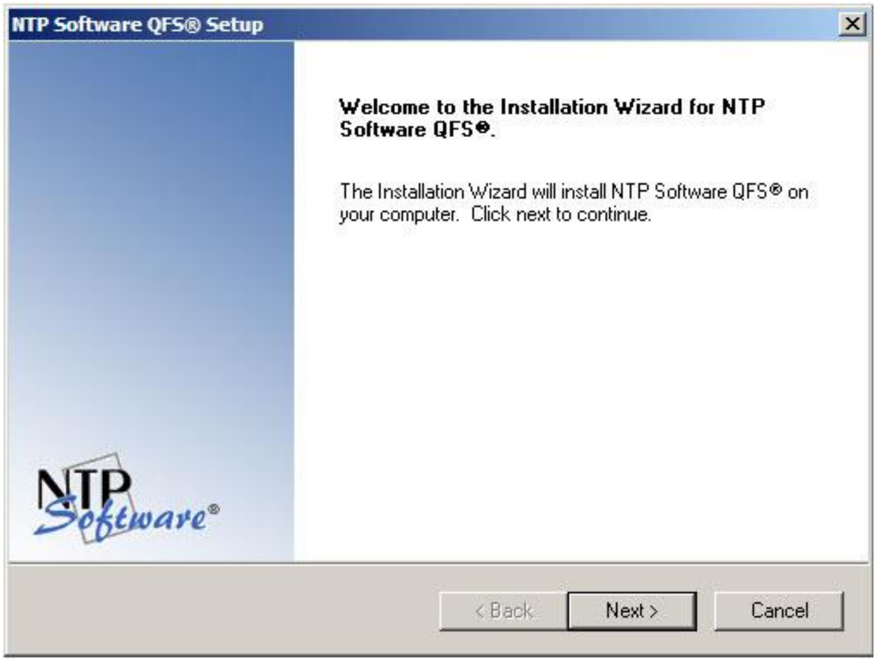
NTP Software Installation Wizard for Smart Policy Manager Complete

The Installation Wizard has successfully installed Smart Policy Manager. Click Finish to exit the wizard.

☑ Yes, I want to view the readme file.

Installing NTP Software QFS Admin Component

1. The NTP Software QFS welcome dialog box pops up automatically. Click **Next** to continue.

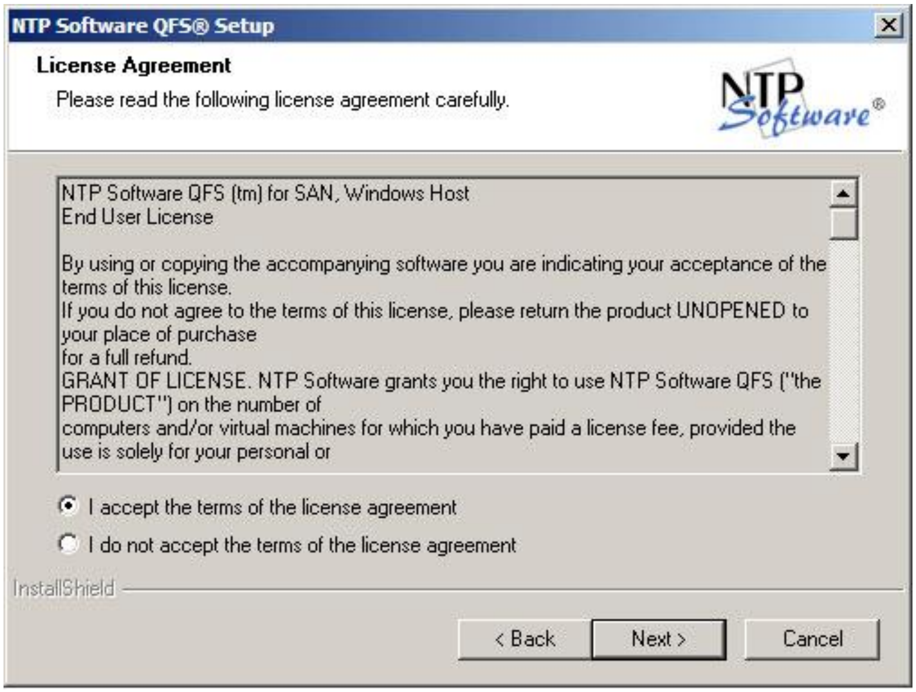


NTP Software QFS® Setup

Welcome to the Installation Wizard for NTP Software QFS®.

The Installation Wizard will install NTP Software QFS® on your computer. Click next to continue.

2. In the **License Agreement** dialog box, select **I accept the terms of the license agreement**, then click **Next**.



NTP Software QFS® Setup

License Agreement

Please read the following license agreement carefully.

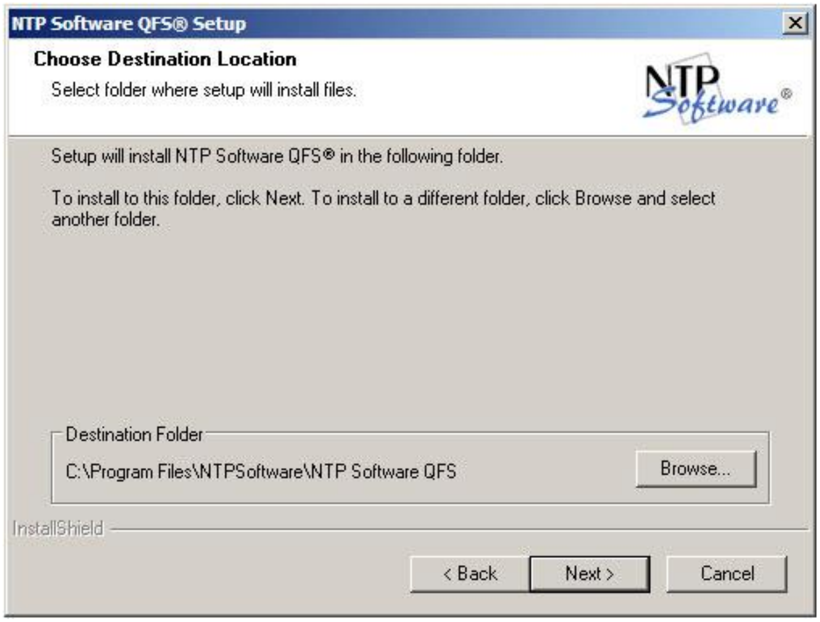
NTP Software QFS (tm) for SAN, Windows Host
End User License

By using or copying the accompanying software you are indicating your acceptance of the terms of this license.
If you do not agree to the terms of this license, please return the product UNOPENED to your place of purchase
for a full refund.
GRANT OF LICENSE. NTP Software grants you the right to use NTP Software QFS ("the PRODUCT") on the number of
computers and/or virtual machines for which you have paid a license fee, provided the use is solely for your personal or

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

3. In the **Choose Destination Location** dialog box, browse to the desired destination, or click **Next** if the default destination location is appropriate.



NTP Software QFS® Setup

Choose Destination Location

Select folder where setup will install files.

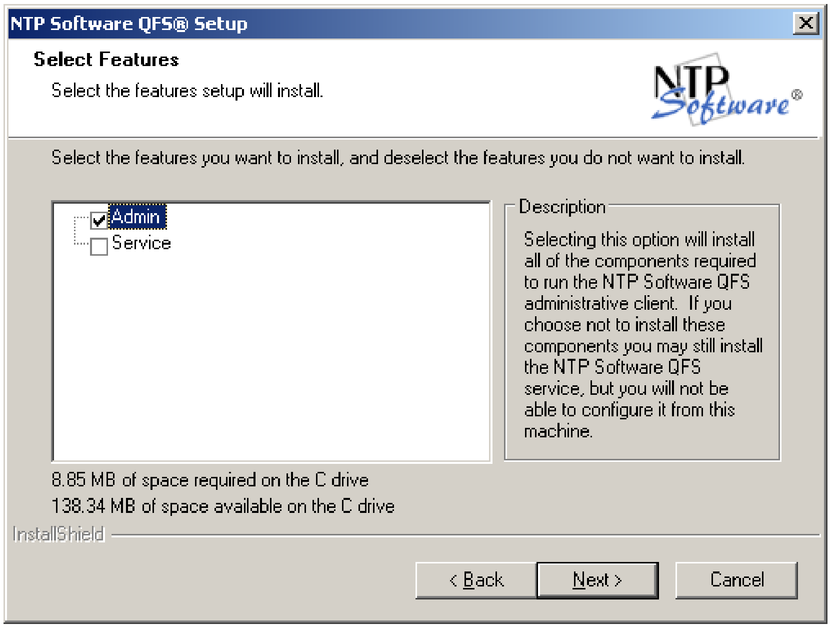
Setup will install NTP Software QFS® in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\NTPSoftware\NTP Software QFS

4. In the **Select Features** dialog box, make sure that only the Admin component is selected; then click **Next**.



NTP Software QFS® Setup

Select Features

Select the features setup will install.

Select the features you want to install, and deselect the features you do not want to install.

☑ Admin
□ Service

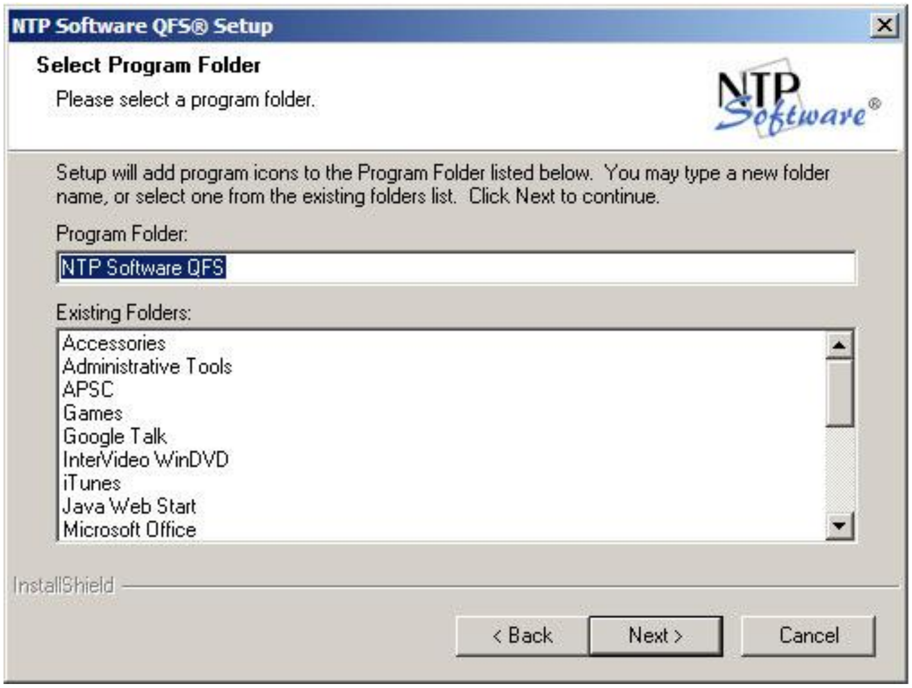
Description

Selecting this option will install all of the components required to run the NTP Software QFS administrative client. If you choose not to install these components you may still install the NTP Software QFS service, but you will not be able to configure it from this machine.

8.85 MB of space required on the C drive
138.34 MB of space available on the C drive

NOTE: Because we just need the Admin User Interface to manage and configure the policies, we checked the Admin Client only. We are not seeking a full NTP Software QFS installation.

5. Specify the program folder (using the default program folder is recommended) and click **Next**. The setup program adds program icons to the program folder.



NTP Software QFS® Setup

Select Program Folder

Please select a program folder.

Setup will add program icons to the Program Folder listed below. You may type a new folder name, or select one from the existing folders list. Click Next to continue.

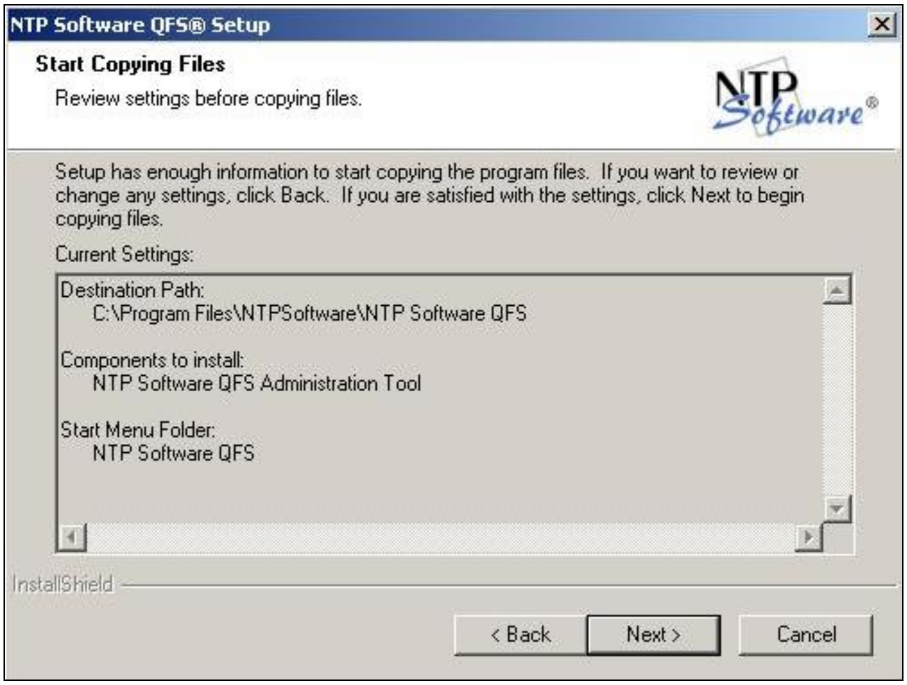
Program Folder:

NTP Software QFS

Existing Folders:

Accessories
Administrative Tools
APSC
Games
Google Talk
InterVideo WinDVD
iTunes
Java Web Start
Microsoft Office

6. Click **Next** when the **Start Copying Files** dialog box appears (assuming that the destination paths are correct). NTP Software QFS setup begins transferring files to the specified locations.



NTP Software QFS® Setup

Start Copying Files

Review settings before copying files.

Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.

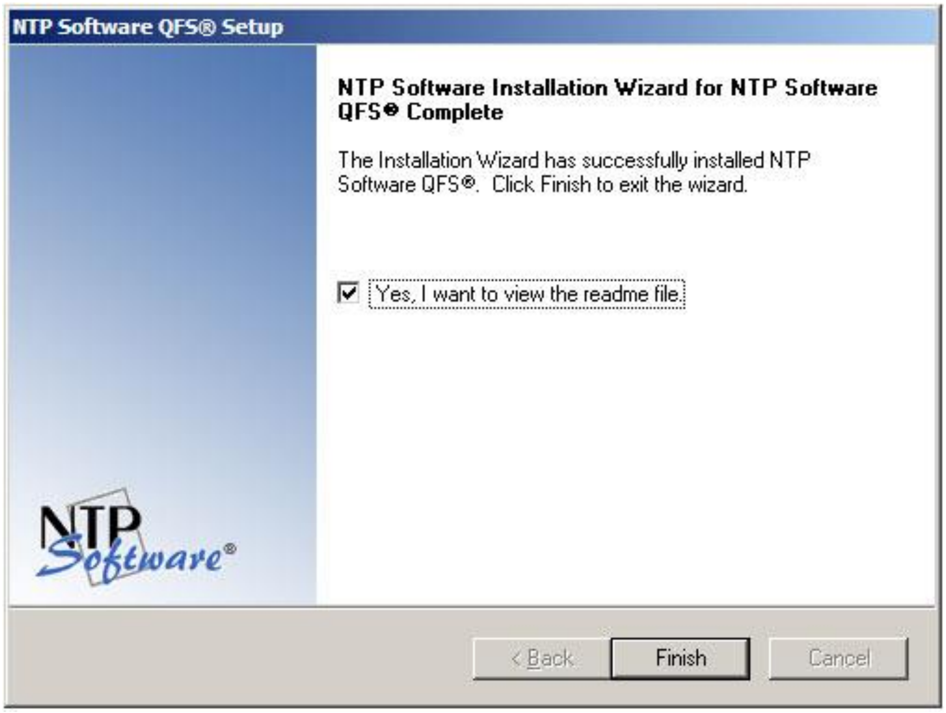
Current Settings:

```
Destination Path:
    C:\Program Files\NTPSoftware\NTP Software QFS

Components to install:
    NTP Software QFS Administration Tool

Start Menu Folder:
    NTP Software QFS
```

7. When the file installation is complete, a dialog box offers you the opportunity to view the readme file. If you do not want to view the readme file at this time, clear the option **Yes, I want to view the readme file**. Click **Finish**. With this step, NTP Software QFS installation is completed.



NTP Software QFS® Setup

NTP Software Installation Wizard for NTP Software QFS® Complete

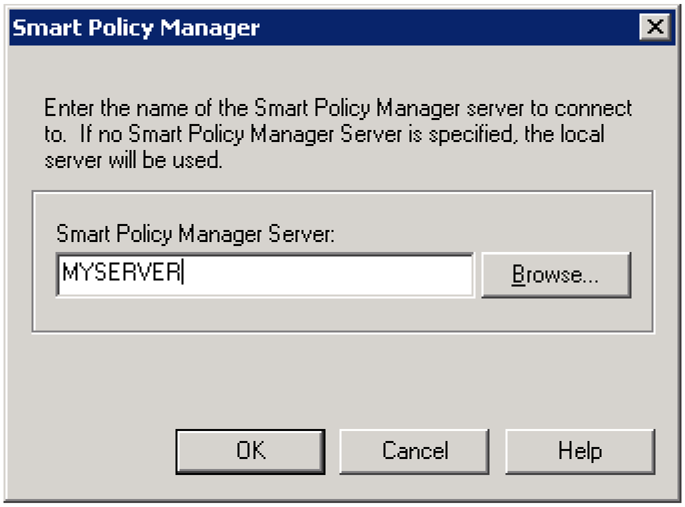
The Installation Wizard has successfully installed NTP Software QFS®. Click Finish to exit the wizard.

☑ Yes, I want to view the readme file.

Administering NTP Software QFS through an NTP Software QFS Admin Client Running on a Different Machine

1. Click **Start** > **Programs** > **NTP Software QFS** > **NTP Software QFS Admin**.

2. On the **Smart Policy Manager** dialog box, specify the Smart Policy Manager Server that you want to connect to.



Enter the name of the Smart Policy Manager server to connect to. If no Smart Policy Manager Server is specified, the local server will be used.

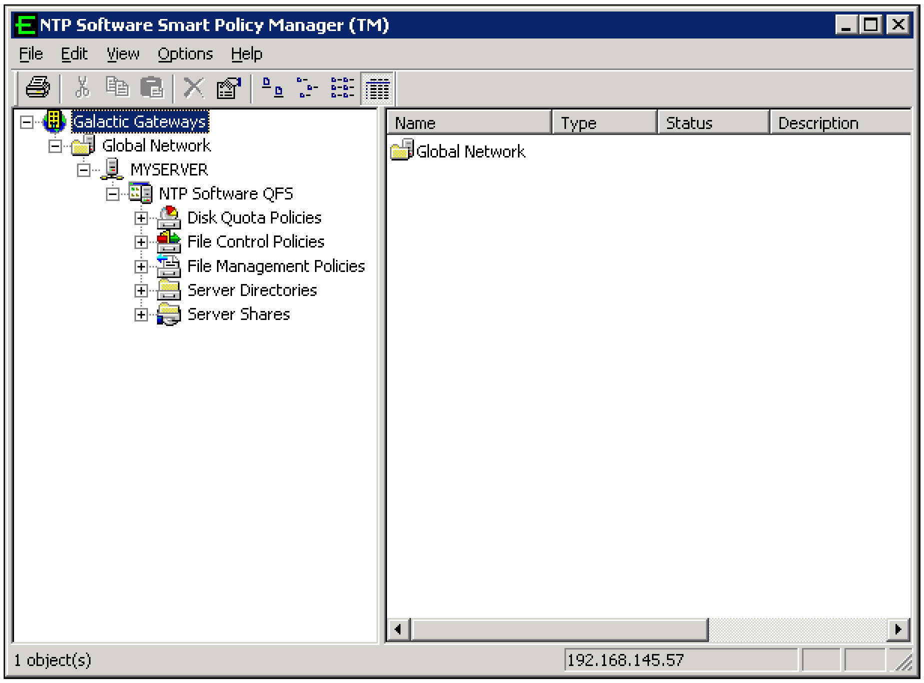
Smart Policy Manager Server: MYSERVER

NOTES:

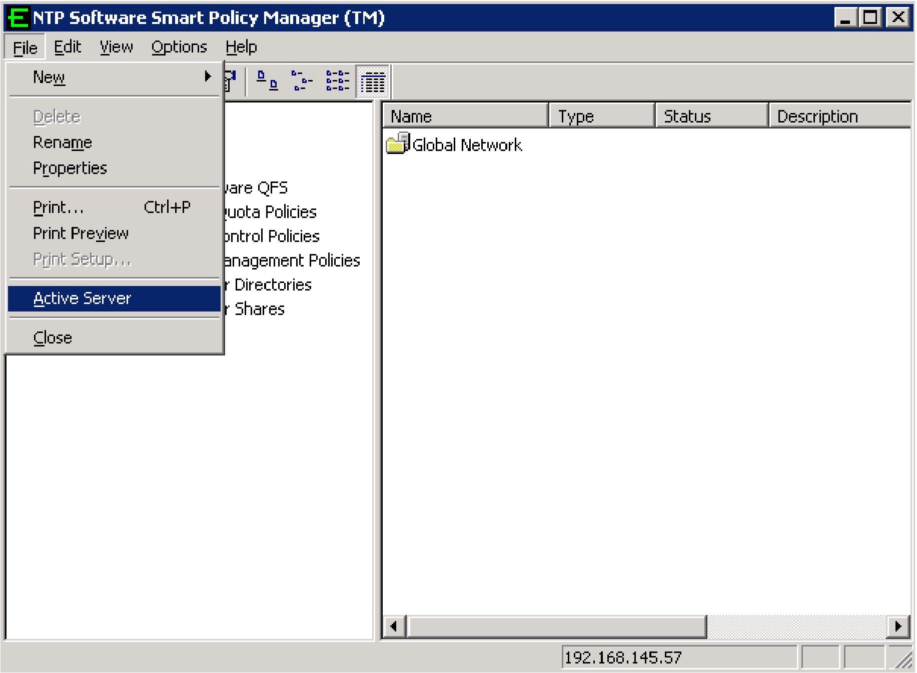
- The Smart Policy Manager Admin component is installed on the local machine so there is no Smart Policy Manager service installed. Thus, NTP Software QFS cannot talk to the local Smart Policy Manager service because it does not exist, so we specify the Smart Policy Manager service that NTP Software QFS should communicate with.

- In very large organizations, you may have offices all over the world. Make sure you connect to the server(s) at reasonable distance to maintain good speed.

As shown, the NTP Software QFS Admin Client User interface is displayed with MYSERVER as a node in the left menu tree and all the NTP Software QFS policy details.



1. To connect to more than one Smart Policy Manager service at the same time, click File > Active Server, then insert the server name or the server IP address. This allows you to add all the servers on your entire network to administer them as needed.



NTP Software QFS Admin Reports

NTP Software QFS has several reporting options for your convenience. We will briefly discuss and demonstrate each option so that you can evaluate them. NTP Software QFS comes installed with a built-in reporting module called NTP Software QFS Admin Reports. To access it and run reports, follow these steps:

1. Click **Start** > **Programs** > **NTP Software QFS for NAS** > **NTP Software QFS for NAS Admin Reports**.

2. The NTP Software Report Wizard appears. Select **Create** a report from a report template and then click **Next**.

3. When prompted to select a report type, click **All Active Quota Policies** and then click **Next**.

4. Select the server(s) for which you want reports. Click the right-arrow **(>)** button to add the selected server(s) to this report and then click **Next**.

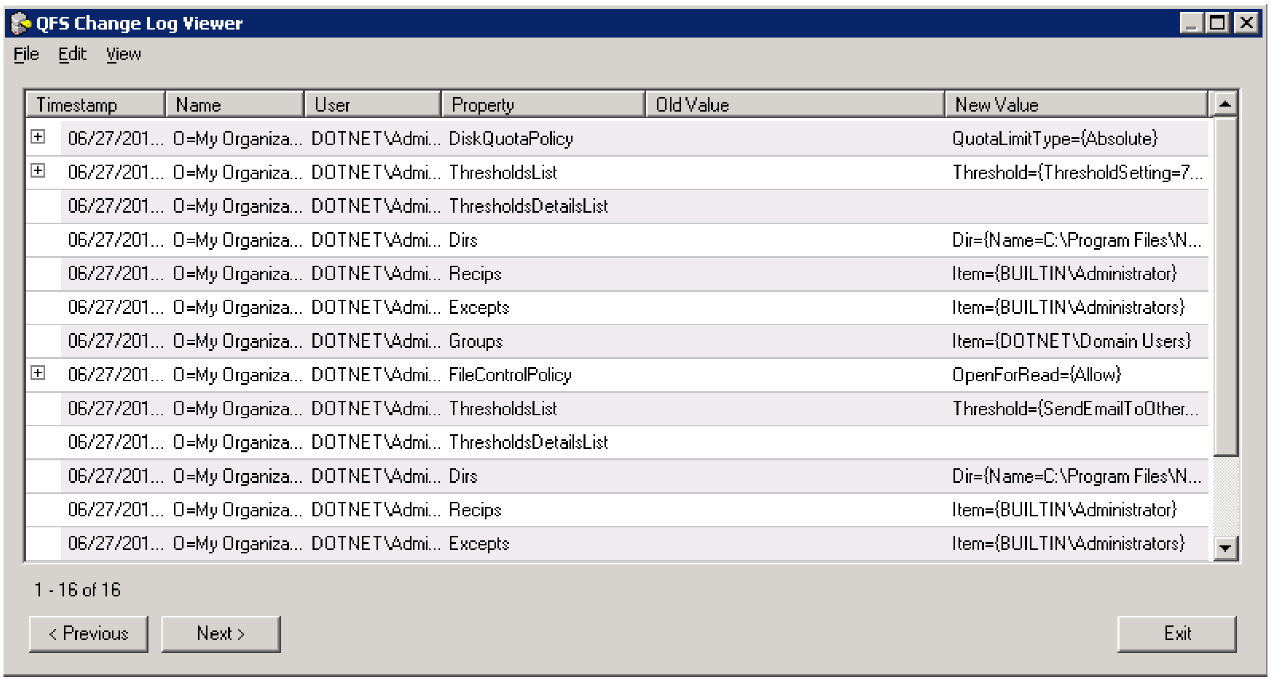
5. Click **Finish** to begin generating the report. The report automatically appears onscreen when complete. When you close the report, you are asked whether you want to save it; if so, specify the desired location.

Viewing QFS Admin Change Log Report

Every change users make through QFS Admin is stored; the old configuration value and the new configuration value for the specific QFS property or policy is logged to the EASE storage. The change log report displays the history of changes occurred in the QFS.

To view the QFS admin change log report:

1. From the **View** menu click **Change Log Report Viewer**



Timestamp	Name	User	Property	Old Value	New Value
⊞ 06/27/201...	O=My Organiza...	DOTNET\Admi...	DiskQuotaPolicy		QuotaLimitType={Absolute}
⊞ 06/27/201...	O=My Organiza...	DOTNET\Admi...	ThresholdsList		Threshold={ThresholdSetting=7...
06/27/201...	O=My Organiza...	DOTNET\Admi...	ThresholdsDetailsList		
06/27/201...	O=My Organiza...	DOTNET\Admi...	Dirs		Dir={Name=C:\Program Files\N...
06/27/201...	O=My Organiza...	DOTNET\Admi...	Recips		Item={BUILTIN\Administrator}
06/27/201...	O=My Organiza...	DOTNET\Admi...	Excepts		Item={BUILTIN\Administrators}
06/27/201...	O=My Organiza...	DOTNET\Admi...	Groups		Item={DOTNET\Domain Users}
⊞ 06/27/201...	O=My Organiza...	DOTNET\Admi...	FileControlPolicy		OpenForRead={Allow}
06/27/201...	O=My Organiza...	DOTNET\Admi...	ThresholdsList		Threshold={SendEmailToOther...
06/27/201...	O=My Organiza...	DOTNET\Admi...	ThresholdsDetailsList		
06/27/201...	O=My Organiza...	DOTNET\Admi...	Dirs		Dir={Name=C:\Program Files\N...
06/27/201...	O=My Organiza...	DOTNET\Admi...	Recips		Item={BUILTIN\Administrator}
06/27/201...	O=My Organiza...	DOTNET\Admi...	Excepts		Item={BUILTIN\Administrators}

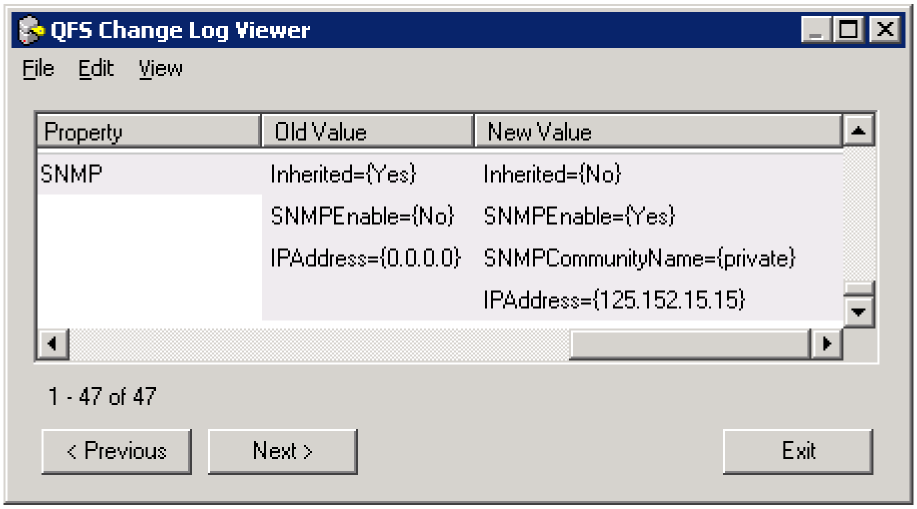
Copyright © 2000-2015 NTP Software

Following is the description of the fields of the change log report:

Field	Description
Timestamp	displays the time of change.
Name	displays the distinguished name of QFS property \ policy upon which changes are applied.
User	displays the domain account of the user who performed the change
Property	displays the short name for the property.
Old Value	displays the old value of the property before applying the change.
New Value	displays the new value of the property after applying the change.

The values displayed within the viewer in both old value and new value columns are describing either primitive property values or composite ones. Primitive properties are those without any special configuration for any of the contained parameters like QFS SMTP, for example. However, composite properties are those that contain configuration for each value of some of its parameters like QFS security configuration property that contain configuration for each security account value.

For primitive properties, each parameter is displayed along with its corresponding value in a separate row.

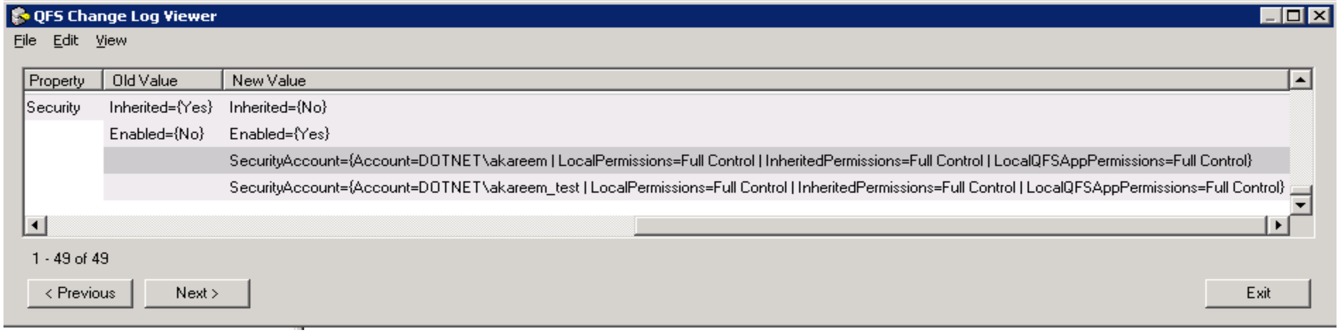


Property	Old Value	New Value
SNMP	Inherited={Yes}	Inherited={No}
	SNMPEnable={No}	SNMPEnable={Yes}
	IPAddress={0.0.0.0}	SNMPCommunityName={private}
		IPAddress={125.152.15.15}

1 - 47 of 47

Copyright © 2000-2015 NTP Software

However, for composite properties, values for composite parameters along with their corresponding related parameters' values are displayed in one row with a vertical bar separating them and values for non-composite parameters are displayed in a single row.



Property	Old Value	New Value
Security	Inherited={Yes}	Inherited={No}
	Enabled={No}	Enabled={Yes}
		SecurityAccount={Account=DOTNET\akareem | LocalPermissions=Full Control | InheritedPermissions=Full Control | LocalQFSAppPermissions=Full Control}
		SecurityAccount={Account=DOTNET\akareem_test | LocalPermissions=Full Control | InheritedPermissions=Full Control | LocalQFSAppPermissions=Full Control}

1 - 49 of 49

Importing/Exporting QFS Admin Change Log Data

QFS change Log Viewer enables QFS users to import change log data to be displayed via the viewer. Data is received in the form of XML for only displaying and does not affect EASE storage of the installed QFS.

Through exporting, change log data is generated in either the form of XML or binary data. The exported data can be displayed via any XML viewer tool or web browser. It can also be imported to another QFS change log viewer installed with another QFS Admin, even outside the organization, to be tracked and explored.

NTP Software QFS for NAS Configuration Wizard

1. Click Start > Programs > NTP Software QFS for NAS > NTP Software QFS for NAS Configuration Wizard.

2. Click the **View Pre-Wizard Checklist** button and gather the required information before continuing. Click **Next**.

3. Enter the name of your NAS device. Click **Next**.

4. If you do not want to send email notifications to users when a quota status changes, clear the **Yes! We do want email notifications enabled** checkbox. Specify which email system your environment uses. Click **Next**.

5. Enter the name of your Active Directory server. (Enter a second server, if desired.) Click the **Test Active Directory Lookup** button and test at least one email address to verify connectivity. Then click **Next**.

6. Enter the SMTP gateway, the SMTP domain, and the email address to use for notifications. Enter any password(s) required for your environment. Click **Test Mail Settings** to verify that the information is correct. Then click **Next**.

7. Click the **Create a Local Policy** button to see how to link the Filer or CIFS Server to NTP Software QFS. Review the remaining information by clicking through the buttons in the lower half of the dialog box. When finished, click **Close**.

> **NOTE:** The NTP Software QFS for NAS Configuration Wizard is also available via the menu. Click **Start > Programs > NTP Software QFS for NAS > NTP Software QFS for NAS Configuration Wizard**.

Requirements

NTP Software provides administrators with the option to perform user administration tasks through the command-line interface. The command-line interface enables administrators to automate routine tasks within NTP Software. Utilizing the command-line interface, an administrator can write a series of commands in a batch file, which can be scheduled to run at regular intervals. With the batch file running, the command-line interface functions as if commands were being entered manually.

Usage

The command-line interface uses the following command structure:

```
QFSCMD <command> <EASE hierarchy path> <command parameters>
```

`<command>` Specifies the name of the command.

`<EASE hierarchy path>` An optional parameter that defines where in the EASE hierarchy the command will apply. By default, all commands apply to the local machine as it appears in the Smart Policy Manager hierarchy.

Example:

```
EASE://My Organization\My Site\W2KCONN\Quota & File Sentinel
```

`<command parameters>` A variable number of command-specific parameters. See the following reference section for details of the parameters for each command.

Example:

```
C:\QFS_CLI\QfsCmd.exe AddQuotaPolicy "EASE://My Organization\My Site\W2KCONN\Quota & File Sentinel" cli_aqp_03 DIR
```

NOTE: When using the command-line console with batch (.BAT) files, the percent sign (%), if used, must be doubled (for example, 90%%).

The following sections provide a complete list of supported commands and parameters.

Copyright © 2000-2015 NTP Software

Quick Reference

The following table briefly describes the commands for policy manipulation. See the **Command Reference** (following) for a complete alphabetical listing of all of the commands, with parameters and descriptions.

Command	**Description**
AddQuotaPolicy	Adds a new quota policy.
AddFileControlPolicy	Adds a new file control policy.
AddFileRemovalPolicy	Adds a new file removal policy.
RemovePolicy	Removes a policy.
AddPolicyDescription	Adds a description for a policy.
AddTargetUsers	Adds users or groups to the list of users governed by a policy.
RemoveTargetUsers	Removes users or groups from the list of users governed by a policy.
AddExemptUsers	Adds users to the list of users exempt from a policy.
RemoveExemptUsers	Removes users from the list of users exempt from a policy.
AddTargetPath	Adds directories or share paths to the list of paths governed by a policy.
RemoveTargetPath	Removes directories or share paths from the list of paths governed by a policy.
SetAlwaysEnforce	Sets the flag indicating whether a policy is always to be enforced.
SetQuotaLimit	Sets the quota limit for a policy.
AddUserThreshold	Adds a user threshold.
AddOwnerThreshold	Adds a quota threshold for the owner of the file.
AddRecipientThreshold	Adds a quota threshold for recipients.
AddOtherRecipientThreshold	Adds a quota threshold for other recipients.
AddThresholdCommand	Adds a threshold command.
RemoveThreshold	Removes a threshold from a policy.
AddOtherRecipients	Adds other recipients to a list.
RemoveOtherRecipients	Removes other recipients from a list.
AddFilePatterns	Adds file patterns for a file blocking policy.
RemoveFilePatterns	Removes file patterns from a file blocking policy.
SetFileControlOptions	Sets the control options for a file blocking policy.
SetEmailMessageFormat	Sets the format for email messages.
SetSmtpConfiguration	Sets SMTP configuration parameters.
SetFileRemovalCriteria	Sets the lifetime for a file removal policy.
SetQuotaDenyWriteLevel	Sets the level at which a quota denies file writes.

Command Reference

AddExemptUsers

Adds a specific user or list of users to the policy's exempt user list.

Syntax

```
AddExemptUsers <targetserver> <policy> <account>
```

Parameters

Parameter name	Description
targetserver	Level of the policy
policy	Name of the policy
users	List of user or group accounts, separated by semicolons

Result

Exempt users <users> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

NOTE: If you have only one user in the list, you do not need to put a semicolon at the end.

Copyright © 2000-2015 NTP Software

AddFileControlPolicy

Creates a new file control policy and adds it to the NTP Software QFS configuration.

Syntax

```
AddFileControlPolicy <targetserver> <policy> <type>
```

Parameters

Parameter name	Description
targetserver	Level of the policy
policy	Name of the file control policy to add
type	DIR — Directory policy SHARE — Share policy

Result

File control policy <policy> successfully added or a text message describing the error encountered.

Remarks

The new policy is created at the level specified by the first parameter. If targetserver is left blank, the policy is created under the local server's NTP Software QFS application level. The policy name must be surrounded by double quotes ("") if it contains a space.

AddFilePatterns

Adds file patterns for a file control policy.

Syntax

```
AddFilePatterns <targetserver> <policy> <patterns>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
patterns	List of file patterns, separated by semicolons.

Result

File patterns <patterns> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

AddFileRemovalPolicy

Creates a new file removal policy and adds it to the NTP Software QFS configuration.

Syntax

```
AddFileRemovalPolicy <targetserver> <policy> <type>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the file removal policy to add.
type	DIR — Directory policy. SHARE — Share policy.

Result

File removal policy <policy> successfully added or a text message describing the error encountered.

Remarks

The new policy is created at the level specified by the first parameter. If targetserver is left blank, the policy is created under the local server’s NTP Software QFS application level. The policy name must be surrounded by double quotes ("") if it contains a space.

Copyright © 2000-2015 NTP Software

AddOtherRecipients

Adds other recipients to the recipient list.

Syntax

```
AddOtherRecipients <targetserver> <policy> <users>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Recipients <users> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

NOTE: If you have only one user in the list, you do not need to put a semicolon at the end.

Copyright © 2000-2015 NTP Software

AddOtherRecipientThreshold

Adds a quota threshold for other recipients.

Syntax

```
AddOtherRecipientThreshold <targetserver> <policy>
<thresholdvalue> <thresholdtype> <abovesubject>
<abovemessage> <aboveemail> <belowsubject> <belowmessage>
<belowemail>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	Email notification. Username pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reaches threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

Other recipient threshold added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It is very important that you specify all the parameters for messages. If you do not want to set any particular message, specify an empty value enclosed in double quotes.

Copyright © 2000-2015 NTP Software

AddOwnerThreshold

Adds a quota threshold for the owner of a file.

Syntax

```
AddOwnerThreshold <targetserver> <policy> <thresholdvalue>
<thresholdtype> <abovesubject> <abovemessage> <aboveemail>
<belowsubject> <belowmessage> <belowemail>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	Email notification. Username pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reaches threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

Owner threshold successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It is very important that you specify all the parameters for messages. If you do not want to set any particular message, specify an empty value enclosed in double quotes.

AddPolicyDescription

Adds a description to a given policy.

Syntax

```
AddPolicyDescription <targetserver> <policy> <description>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
description	Description to be assigned to the policy.

Result

Policy description <description> successfully added to policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

AddQuotaPolicy

Creates a new quota policy and adds it to the NTP Software QFS configuration.

Syntax

```
AddQuotaPolicy <targetserver> <policy> <type>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the quota policy to add.
type	DIR — Directory policy. SHARE — Share policy.

Result

Quota policy <policy> successfully added or a text message describing the error encountered.

Remarks

The new policy is created at the level specified by the first parameter. If targetserver is left blank, the policy is created under the local server’s NTP Software QFS application level. The policy name must be surrounded by double quotes ("") if it contains a space.

AddRecipientThreshold

Adds a recipient threshold for the given policy.

Syntax

```
AddRecipientThreshold <targetserver> <policy>
<thresholdvalue> <thresholdtype> <abovesubject>
<abovemessage> <aboveemail> <belowsubject> <belowmessage>
<belowemail>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
thresholdtype	Email notification. Username pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reached threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

Recipient threshold successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It is very important that you specify all the parameters for messages. If you do not want to set any particular message, specify an empty value enclosed in double quotes.

AddTargetPath

Adds one or more specific directories or share paths to the list of paths governed by the policy.

Syntax

```
AddTargetPath <targetserver> <policy> <path>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
path	List of folder paths, separated by semicolons.

Result

Target path <path> successfully added to the target path <path> or a text message describing the error encountered.

Remarks

The target path(s) must be surrounded by double quotes ("") if the path contains a space.

AddTargetUsers

Adds a specific user or group to the list of users governed by the policy.

Syntax

```
AddTargetUsers <targetserver> <policy> <users>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Target users <users> successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes. Note: If you have only one user in the list, you do not need to put a semicolon at the end.

AddThresholdCommand

Adds a threshold command to be executed when the user goes above or below threshold value.

Syntax

```
AddThresholdCommand <targetserver> <policy>
<thresholdvalue> <abovecommand> <belowcommand>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.
abovecommand	Command to be executed when user goes above threshold.
belowcommand	Command to be executed when user goes below threshold.

Result

Threshold command successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It is very important that you specify all the parameters for messages. If you do not want to set any particular message, specify an empty value enclosed in double quotes.

AddUserThreshold

Adds a user threshold to the policy.

Syntax

```
AddUserThreshold <targetserver> <policy> <thresholdvalue>
<thresholdtype> <abovesubject> <abovemessage> <aboveemail>
<belowsubject> <belowmessage> <belowemail>
```

Parameters

Parameter name	**Description**
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	value at which the threshold will be triggered.
thresholdtype	1 — Email notification. 2 — Username pop-up. 3 — Computer name pop-up.
abovesubject	Subject of notification message showing user has reached threshold.
abovemessage	Body of notification message showing user has reached threshold.
aboveemail	Body of email notification message showing user has reached threshold.
belowsubject	Subject of notification message showing user has gone below threshold.
belowmessage	Body of notification message showing user has gone below threshold.
belowemail	Body of email notification message showing user has gone below threshold.

Result

User threshold successfully added to the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0. Enclose all messaging parameters in double quotes. It is very important that you specify all the parameters for messages. If you do not want to set any particular message, specify an empty value enclosed in double quotes.

RemoveExemptUsers

Removes a specific user or list of users from the policy's exempt user list.

Syntax

```
RemoveExemptUsers <targetserver> <policy> <users>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Exempt users <users> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

NOTE: If you have only one user in the list, you do not need to put a semicolon at the end.

RemoveFilePatterns

Removes file patterns from a file control policy.

Syntax

```
RemoveFilePatterns <targetserver> <policy> <patterns>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
patterns	List of file patterns, separated by semicolons.

Result

File patterns <patterns> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

> **NOTE:** If you have only one user in the list, you do not need to put a semicolon at the end.

Copyright © 2000-2015 NTP Software

RemoveOtherRecipients

Removes other recipients from the recipient list.

Syntax

```
RemoveOtherRecipients <targetserver> <policy> <users>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Other recipients <users> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

NOTE: If you have only one user in the list, you do not need to put a semicolon at the end.

RemovePolicy

Removes a policy from the NTP Software QFS configuration.

Syntax

```
RemovePolicy <targetserver> <policy>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.

Result

Policy <policy> successfully removed or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

Copyright © 2000-2015 NTP Software

RemoveTargetPath

Removes one or more specific directories or share paths from the list of paths governed by the policy.

Syntax

```
RemoveTargetPath <targetserver> <policy> <path>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
path	List of folder paths, separated by semicolons.

Result

Policy <policy> successfully removed or a text message describing the error encountered.

Remarks

The target path(s) must be surrounded by double quotes ("") if the path contains a space.

RemoveTargetUsers

Removes a specific user or group from the list of users governed by the policy.

Syntax

```
RemoveTargetUsers <targetserver> <policy> <users>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
users	List of user or group accounts, separated by semicolons.

Result

Target users <users> successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. It is very important that you specify the list enclosed in double quotes.

NOTE: If you have only one user in the list, you do not need to put a semicolon at the end.

RemoveThreshold

Removes a threshold from the policy.

Syntax

```
RemoveThreshold <targetserver> <policy> <thresholdvalue>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
thresholdvalue	Threshold value at which the threshold will be triggered.

Result

Threshold successfully removed from the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space. The threshold value should be greater than 0.

Copyright © 2000-2015 NTP Software

SetAlwaysEnforce

Sets the flag indicating whether the policy is always to be enforced.

Syntax

```
SetAlwaysEnforce <targetserver> <policy> <flag>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
flag	0 — Policy is not always enforced. 1 — Policy is always enforced.

Result

Always Enforce Flag successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetEmailMessageFormat

Specifies the format of the threshold email message.

Syntax

```
SetEmailMessageFormat <targetserver> <policy> <format>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
flag	0 — Plaintext format. 1 — Rich text format.

Result

Email message format successfully set to <format> or a text message describing the error encountered.

Remarks

None.

Copyright © 2000-2015 NTP Software

SetFileControlOptions

Sets the control options for a file control policy.

Syntax

```
SetFileControlOptions   <targetserver>   <policy>   <rwoption>
<croption>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
rwoption	Option for the read/write flag: 0 — Allow read/write. 1 — Log event for read/write. 2 — Deny read/write.
croption	Option for the file creation flag: 0 — Allow create. 1 — Log event for create. 2 — Deny file creation.

Result

File control options successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetFileRemovalCriteria

Sets criteria for a file removal policy.

Syntax

```
SetFileRemovalCriteria <targetserver> <policy>
<durationtype> <duration> <deletepreexisting>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
durationtype	0 — Hours 1 — Days 2 — Weeks 3 — Months
duration	Duration value. Should be greater than 0 and less than 65535.
deletepreexisting	0 — Do not delete existing files. 1— Delete existing files.

Result

File removal criteria successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetQuotaDenyWriteLevel

Sets the level at which writes will be denied.

Syntax

```
SetQuotaDenyWriteLevel <targetserver> <policy> <level>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
level	Percentage level at which to deny writes. Must be between 0 and 200.

Result

Quota 'Deny Write Level' for policy <policy> successfully set to <level> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

SetQuotaLimit

Sets the quota limit for the policy.

Syntax

```
SetQuotaLimit <targetserver> <policy> <limit>
```

Parameters

Parameter name	Description
targetserver	Level of the policy.
policy	Name of the policy.
limit	Quota limit value, in megabytes (MB). This value should be greater than 0.

Result

Quota limit successfully set for the policy <policy> or a text message describing the error encountered.

Remarks

The policy name must be surrounded by double quotes ("") if it contains a space.

Copyright © 2000-2015 NTP Software

SetSmtpConfiguration

Sets the SMTP configuration parameters for targetserver.

Syntax

```
SetSmtpConfiguration
<targetserver><inheritemailconfiguration>   <enable/disable>
<smtpserver> <smtpdomain> <senderaddress> <senderpassword>
```

Parameters

Parameter name	Description
targetserver	Level at which the policy needs to be created within the EASE hierarchy.
inheritemailconfiguration	0 — Do not inherit email configuration. 1 — Inherit email configuration.
enable/disable	0 — Enable 1 — Disable
smtpserver	SMTP server name or IP address.
smtpdomain	Domain for SMTP server.
senderaddress	Email address to be set in the To field of the email message.
senderpassword	Password for the sender’s address.

Result

(SMTP) configuration set successfully or a text message describing the error encountered.

Remarks

None.

Appendix:

- NTP Software QFS requires a manual setup by an administrator for clustered environments.

- The Connector service can be started on the servers on which NTP Software QFS was installed; however, in the NTP Software QFS user interface, the Filer or CIFS Server is assigned to only one server node and must be reassigned manually from a previously assigned node.

- A Filer or CIFS Server cannot communicate with more than one NTP Software QFS server at a time.

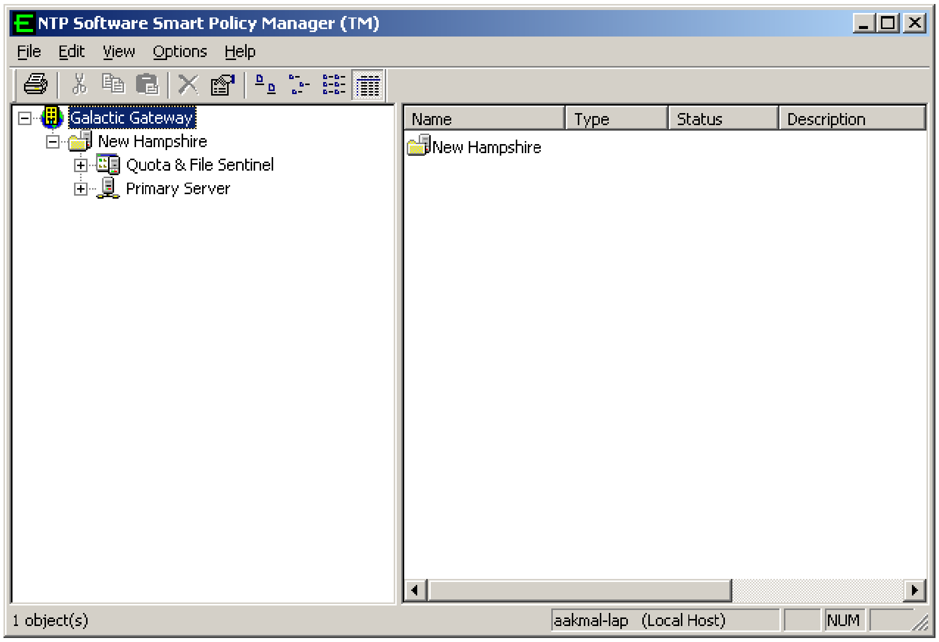
Installing NTP Software QFS in Clustered Environments

1. Install NTP Software QFS on a server as described in NTP Software QFS for NAS, EMC Edition Quick Start Guide, ID #6051EF.

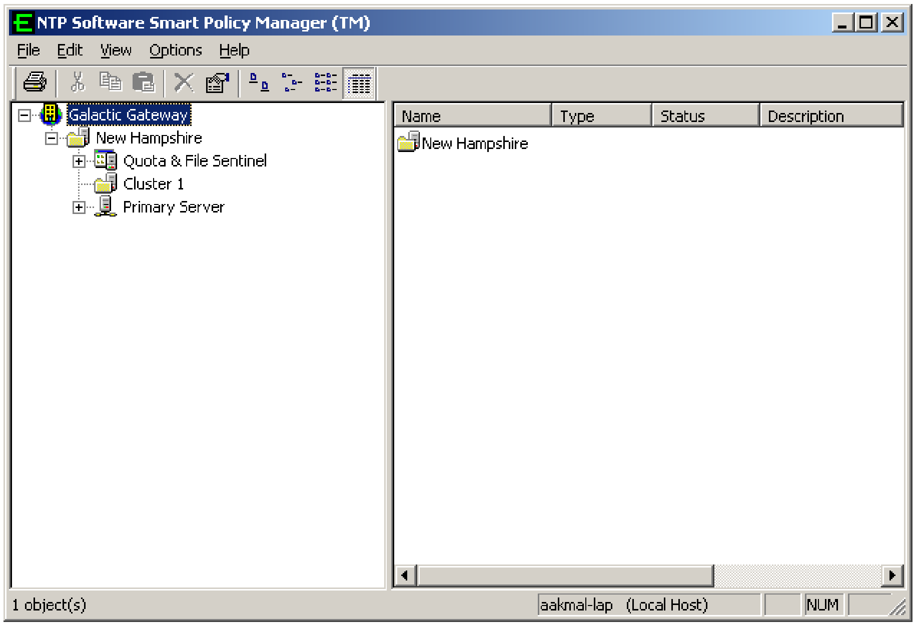
2. After NTP Software QFS is installed successfully, open NTP Software QFS to find the global container (in this example, Galactic Gateway) at the top of the hierarchy. Click the plus sign (+) to expand the container.

3. Click the plus sign (+) to expand your site container (in this example, New Hampshire) in the second tier of the hierarchy.

   Notice the installation server (in this example, Primary Server) in the third tier of the hierarchy. The NTP Software QFS application is also in the third tier.



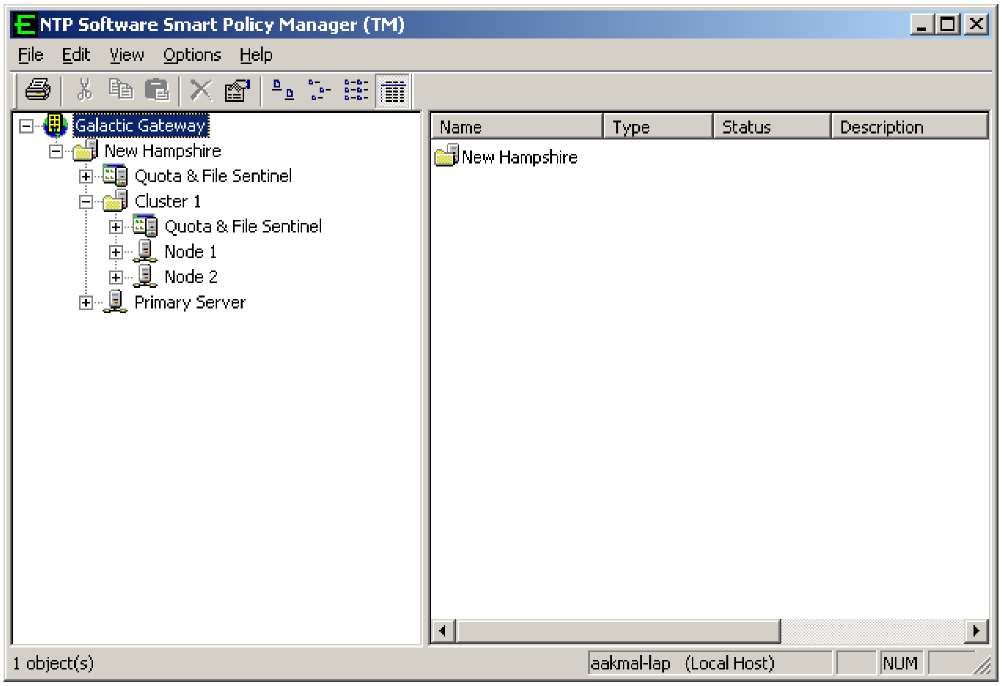
4. Right-click the site container (New Hampshire in this example) and then select New > Container from the pop-up menu to create your cluster container. Give the new container the name of the cluster. In the example, we have used Cluster 1 as the name.



5. Right-click the cluster container (Cluster 1 in this example) and select New > Quota & File Sentinel Application from the pop-up menu.

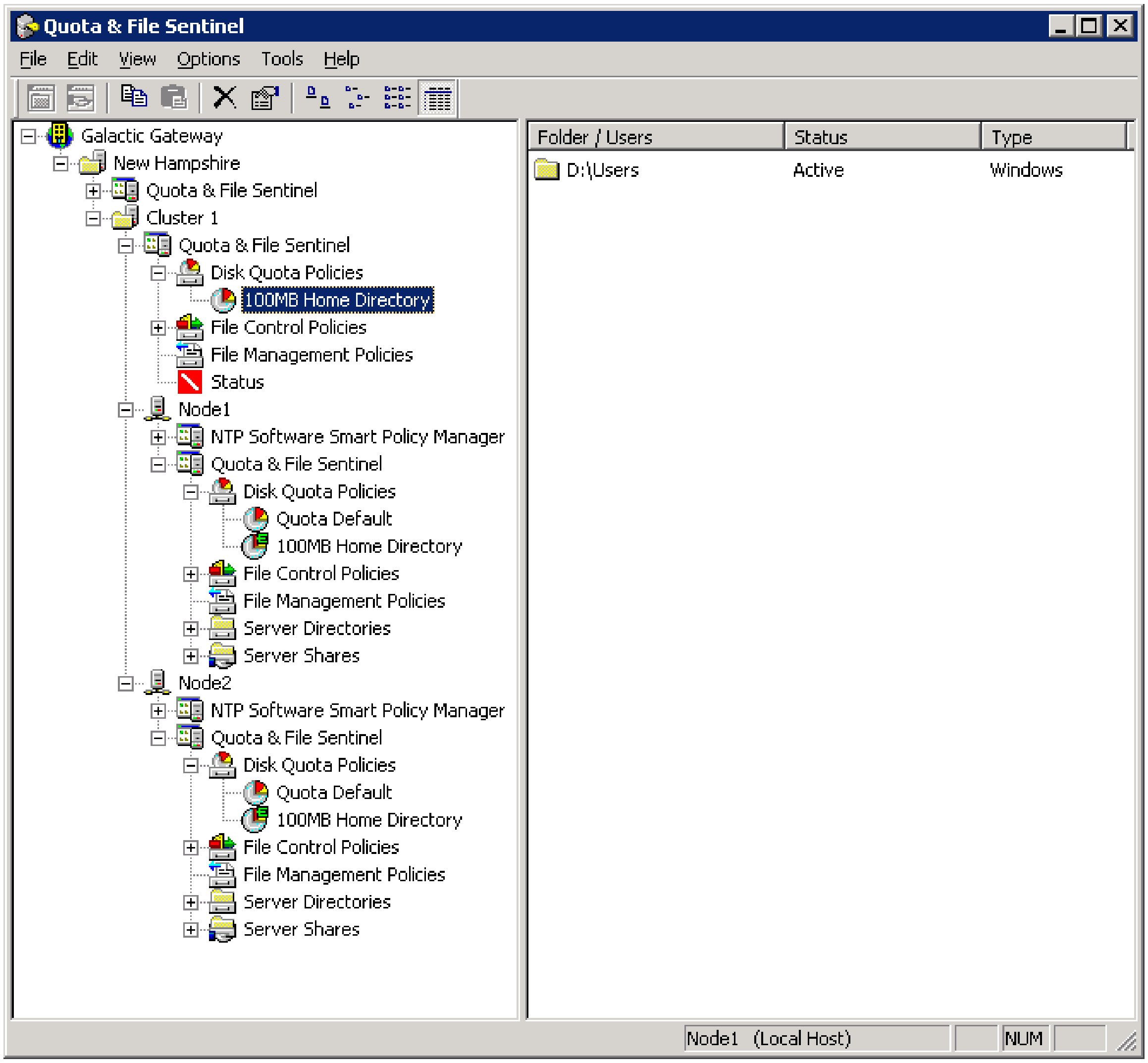
   It is necessary to install NTP Software QFS manually on each server you want to add to the tree (Node 1 and Node 2 in this example). Choose the option Adding to an enterprise installation during the local NTP Software Smart Policy Manager installation on each node, and point to the first NTP Software QFS server.

6. Open the cluster container in the NTP Software Smart Policy Manager hierarchy and use the drag-and-drop method to move the nodes into the cluster container. They will appear at the same level as the container Quota & File Sentinel application, as shown here.



Click the plus sign (+) next to the NTP Software QFS application you have just added, to view the global (cluster) policies. Create all policies within this application that will be applied to both nodes. They will be propagated automatically to all nodes within the container.

In the following example, the global 100MB policy is propagated. The replicated policies are denoted by the green E on the icon within each node.



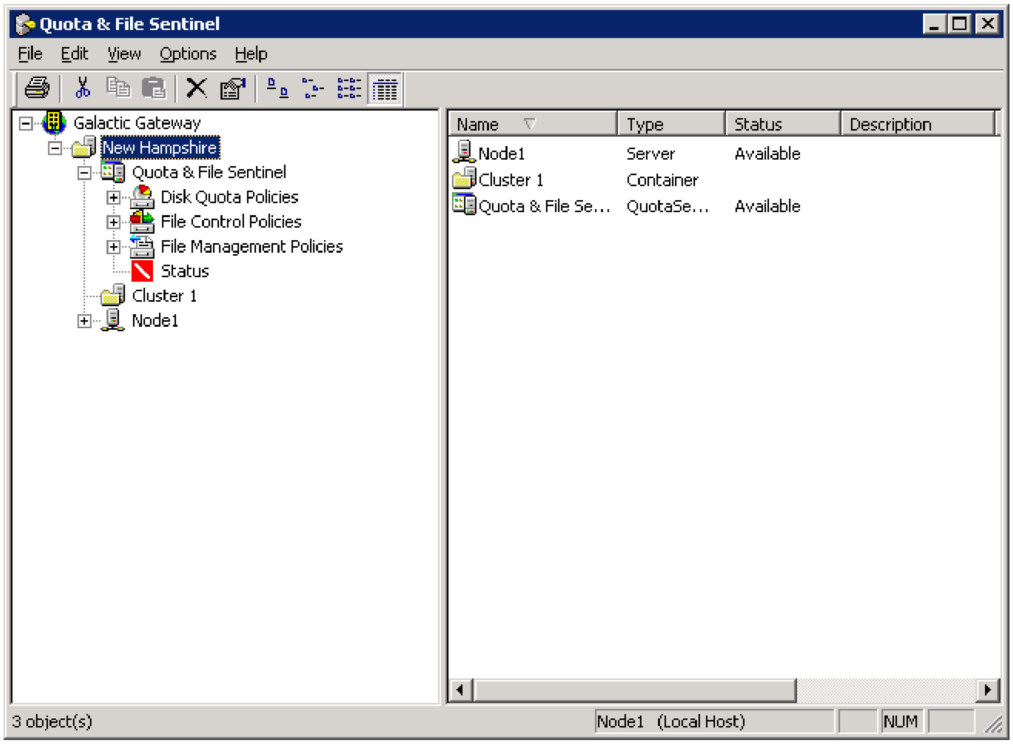
Folder / Users	Status	Type
D:\Users	Active	Windows

Installing NTP Software QFS onto a Node Server

This feature enables administrators to group servers, Filers, and CIFS Servers logically to reflect their organizational physical structure, creating policies under a node that can be inherited by all the machines of that node.

1. It is necessary to install NTP Software QFS manually on each of the added nodes (in this example, on Node 1). Choose the option Adding to an enterprise installation during the local NTP Software Smart Policy Manager installation.

2. Right-click the site container and select New > Container to create a container for the cluster. Give the new container the cluster name.



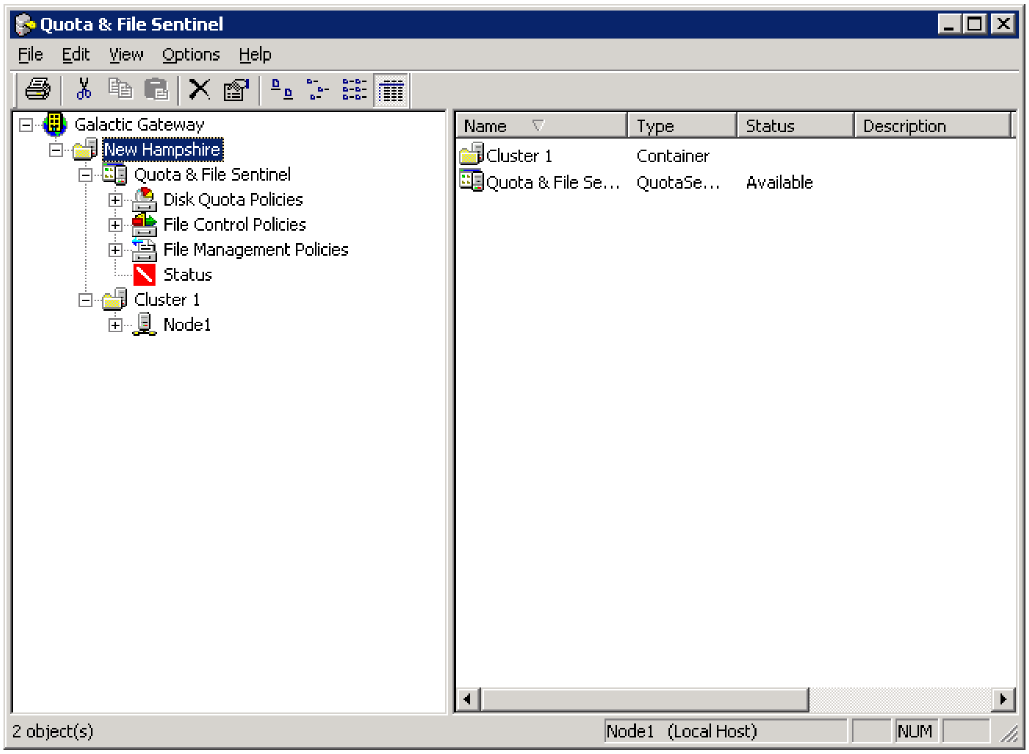
Name	Type	Status	Description
Node1	Server	Available	
Cluster 1	Container		
Quota & File Se...	QuotaSe...	Available	

3. Click the existing server (Node1) and, while holding down the mouse button, drag-and-drop the server onto the cluster container to move the server into the cluster hierarchy.

4. Right-click the cluster container and select New > Quota & File Sentinel Application from the pop-up menu.

Copyright © 2000-2015 NTP Software

5. To view the global (cluster) policies, click the plus sign (+) next to the NTP Software QFS application you have just added.



Name	Type	Status	Description
Cluster 1	Container		
Quota & File Se…	QuotaSe…	Available	

Create all policies within this application that will be applied to both nodes. They will be propagated down automatically to all nodes within the container.

Copyright © 2000-2015 NTP Software

Enabling Data ONTAP fPolicy Management Service

A. In 7-Mode

Perform the following steps to enable the Data ONTAP fpolicy management service:

1. Log on to the NetApp Filer with an account that has administrative privileges.
2. At the prompt, enter the following command:

   ```
   fpolicy create NTPSoftware_QFS screen
   ```

3. Enter the following command:

   ```
   fpolicy enable NTPSoftware_QFS
   ```

4. To verify that CIFS file policies are now enabled, enter the following command:

   ```
   fpolicy
   ```

These steps create the configuration that allows NTP Software QFS to register with and manage your Filer. They must be completed before you try to configure NTP Software QFS. Later in this document, we will register a file policy server with the Filer. No further Filer administration is required.

B. In Cluster Mode

Perform the following steps to enable the Data ONTAP fpolicy management service:

1. Log on to the NetApp server with an account that has administrative privileges.

2. At the prompt, enter the following commands:

   fpolicy policy event create -vserver <*vserver name*> -event-name **NTPSoftware_QFSEVT** -protocol cifs -file-operations close, create, create_dir, rename, rename_dir, delete, delete_dir, read, write, open

   fpolicy policy external-engine create -vserver <*vserver name*> -engine-name **NTPSoftware_QFSENG** -primary-servers <*QFS connector machine IP addresses separated by comma*> -port <*unused dynamic port number*> -extern-engine-type synchronous -ssl-option no-auth

   fpolicy policy create -vserver <*vserver name*> -policy-name **NTPSoftware_QFS** -events **NTPSoftware_QFSEVT** -engine **NTPSoftware_QFSENG** -is-mandatory false -allow-privileged-access yes -privileged-user-name <*QFS connector service domain user account, in the format NetBiosName\UserName*>

   fpolicy policy scope create -vserver <*vserver name*> -policy-name **NTPSoftware_QFS** -shares-to-include "*" -volumes-to-include "*"

   fpolicy enable -vserver <*vserver name*> -policy-name **NTPSoftware_QFS** -sequence-number <*unused sequence number*>

3. To verify that CIFS file policies are now enabled, enter the following command:

   fpolicy show -vserver <*vserver name*>

NOTES:

- QFS will create and enable fpolicy automatically for the managed CIFS Server on the cluster-mode Filer using default sequence number 1. Since sequence number cannot duplicate.
- QFS will fail to enable fpolicy on cluster-mode Filer if the sequence number is used by another fpolicy on the same VServer.
- QFS will create a registry value named “***<CifsServerName>*****_FPolicySeqNum**” inside the connector registry key, with default value 1. If QFS failed to enable fpolicy due to a redundant sequence number, then the user can configure this registry value to any unused sequence number, and run the **Diagnose** process on the managed CIFS server from QFS Admin (on the CIFS server Status node).
- The **Diagnose** process will try to enable the fpolicy automatically using the new sequence number configured in registry.

Assign Permissions to User Account to Execute cDOT APIs

In order to manage CIFS server on a cDOT filer, you need to provide user name and password for a Unix user on the cDOT filer with specific permissions. The following steps show how to create a Unix user on the cDOT filer, and how to assign this user account the required permissions to manage CIFS servers on that cDOT filer:

1. Create Unix user on the cDOT filer:
    - unix-user create -vserver *<vserver name>* -user *<user name>* -id *<user id>* -primary-gid *<primary group id>* -full-name *<user full name>*
2. Create the required role that contains the required permissions:

    Note: The role name specified in all of the following commands must be the same, in order to assign this one role at the end to the Unix user you just created by the command above.

    - security login role create -role *<role name>* -cmddirname "network interface show" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "version" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "volume show" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "vserver show" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "vserver cifs show" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "vserver fpolicy policy" -access all -query ""
    - security login role create -role *<role name>* -cmddirname "vserver fpolicy show-engine" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "vserver fpolicy show" -access readonly -query ""
    - security login role create -role *<role name>* -cmddirname "vserver fpolicy enable" -access all -query ""
    - security login role create -role *<role name>* -cmddirname "vserver fpolicy disable" -access all -query ""
    - security login role create -role *<role name>* -cmddirname "vserver fpolicy engine-connect" -access all -query ""
    - security login role create -role *<role name>* -cmddirname "vserver name-mapping" -access all -query ""

- security login role create -role <*role name*> -cmddirname "vserver services unix-user show" -access readonly -query ""

3. Assign the role you created in step #2 to the user you created in step #1:

   - security login create -username <*user name*> -application ontapi -authmethod password -role <*role name*>

Note: When you execute the command above, the filer will ask you to enter, and confirm, a password for that user. The password you enter here will be used along with the user name in QFS Admin/Wizard UI, when you are adding the CIFS server to be managed by QFS.

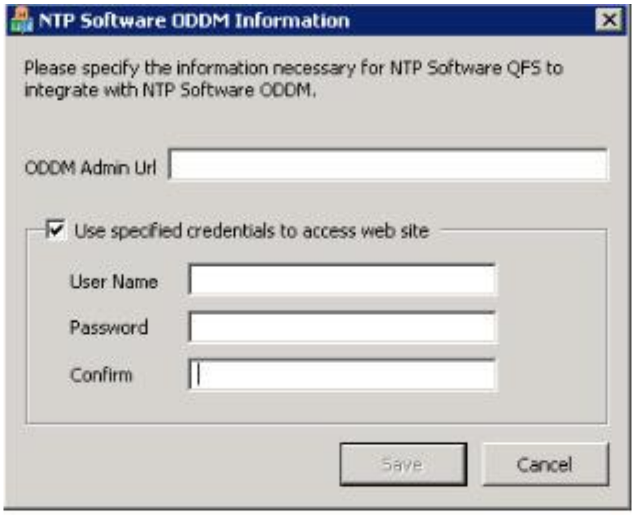
Copyright © 2000-2015 NTP Software

NTP Software QFS and NTP Software On-Demand Data Movement™ (ODDM) Integration

The integration between NTP Software QFS for NetApp and NTP Software ODDM allows NTP Software QFS to manage folder sizes when QFS is configured to use physical sizing versus logical sizing.

To configure the integration, the utility SetODDMInfo is used. The utility is located in the NTP Software QFS installation folder and is launched by double clicking the file through Windows explorer.

NTP Software QFS requires the URL of the NTP Software ODDM Admin website. Once the configuration information has been saved, NTP Software QFS will automatically get the rest of the configuration data from ODDM to integrate the products.



NTP Software ODDM Information

Please specify the information necessary for NTP Software QFS to integrate with NTP Software ODDM.

ODDM Admin Url

☑ Use specified credentials to access web site

User Name

Password

Confirm

. **NOTES:**

- If using Windows Server with Enhanced IE Security enabled, QFS requires credentials to access the ODDM admin site.
- The integration works only if QFS is managing folders by physical size. It has no impact on QFS managing folders by logical size.

About NTP Software

NTP Software is the leading worldwide provider of software solutions for controlling file data across a global infrastructure or at a single site with individual systems. NTP Software delivers a single solution across the entire data storage environment all the way down to the individual user and supports most popular file data storage models and brands. NTP Software products reduce the cost and complexity associated with the exponential growth of unstructured data. NTP Software has been chosen to control file data for the majority of Fortune 1000 companies and thousands of customers in private and public sectors by providing leadership through superior products, services, and experience.

NTP Software Professional Services

NTP Software's Professional Services offers consulting, training, and design services to help customers with their storage management challenges. We have helped hundreds of customers to implement cost-effective solutions for managing their storage environments. Our services range from a simple assessment to in-depth financial analyses.

For further assistance in creating the most cost-effective Storage Management Infrastructure, please contact your NTP Software Representative at 800-226-2755 or 603-622-4400.

The information contained in this document is believed to be accurate as of the date of publication. Because NTP Software must constantly respond to changing market conditions, what is here should not be interpreted as a commitment on the part of NTP Software, and NTP Software cannot guarantee the accuracy of any information presented after the date of publication.

This user manual is for informational purposes only. NTP SOFTWARE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

NTP Software and other marks are either registered trademarks or trademarks of NTP Software in the United States and/or other countries. Other product and company names mentioned herein may be the trademarks of their respective owners.

NTP Software products and technologies described in this document may be protected by United States and/or international patents.

NTP Software
20A NW Boulevard #136
Nashua, NH 03063
Toll Free: 800-226-2755
International: 1-603-622-4400
E-mail: info@ntpsoftware.com
Web Site: http://www.ntpsoftware.com

Copyright © 2015 NTP Software. All rights reserved. All trademarks and registered trademarks are the property of their respective owners. Doc#4829EF